



JOANA AURORA PINHEIRO DA SILVA MASSANO FERREIRA

O DIREITO À PROTEÇÃO DE DADOS EM REDE NO ÂMBITO DA UNIÃO EUROPEIA

Dissertação com vista à obtenção
do grau de Mestre em Direito
Internacional e Europeu

Orientadora:

Doutora Maria Helena Brito, Professora da Faculdade de Direito da Universidade
Nova de Lisboa

Junho de 2017



JOANA AURORA PINHEIRO DA SILVA MASSANO FERREIRA

O DIREITO À PROTEÇÃO DE DADOS EM REDE NO ÂMBITO DA UNIÃO EUROPEIA

Dissertação com vista à obtenção
do grau de Mestre em Direito
Internacional e Europeu

Orientadora:

Doutora Maria Helena Brito, Professora da Faculdade de Direito da Universidade
Nova de Lisboa

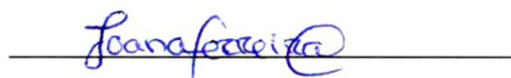
Junho de 2017

Declaração de Compromisso de Anti-Plágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 13 de junho de 2017

Joana Ferreira



Agradecimentos

A elaboração desta dissertação não teria sido possível sem certos apoios inestimáveis e aos quais agradeço de alma e coração.

À minha Orientadora, a Professora Maria Helena Brito, por toda a compreensão, apoio e sabedoria com que me seguiu durante todos estes meses, e sem a qual teria sido impossível concretizar este trabalho.

Aos meus Pais, pelo esforço que sempre encetaram para a realização dos meus sonhos, pela paciência que tiveram a cada momento e pelo incentivo que me deram para que eu nunca desistisse.

À minha Irmã, por sempre encontrar uma alegria quando tudo parece tão negro.

Ao Nuno Viola por todo o amor, companheirismo e amparo quando mais precisei.

À Cristina Cortiço por me apoiar incondicionalmente e tudo fazer para me proporcionar um sorriso.

Às minhas amigas Anabela Brízido, Isabel Seoane, Monnike Montana, Raquel Damião, Rita Carmo e Telma Gonçalves que, com tanta paciência, me auxiliaram em toda esta fase e cujo apoio foi crucial.

Ao Departamento dos Assuntos Jurídicos do Ministério dos Negócios Estrangeiros, pelo carinho com que me acolheram e pelo conhecimento que me transmitiram, em particular à Dra. Inês Matos, pela compreensão constante que me concedeu, e à Dra. Ana Costa Pereira, pela simpatia com que me esclareceu inúmeras dúvidas e me concedeu um “*Lumus*” sempre que a luz parecia apagar-se.

Por último, à Emma, um agradecimento especial, por me ter acompanhado nos estudos desde que me lembro, sempre cheia de ternura e carinho e que, mesmo sem saber, contribuiu decisivamente para quem sou e para a realização dos meus sonhos. Um “adeus” nunca será suficiente para apagar a marca que deixaste em mim.

Modo de Citar e Outros Esclarecimentos

1. O modo de citar segue o disposto nas Normas Portuguesas n.º 405-1 e 405-4 homologadas pelo Instituto Português da Qualidade.
2. As monografias são citadas com referência ao autor, título, local de publicação, editora, ano e página. No texto, a partir da segunda citação, é apenas feita referência a autor, título e página.
3. Os artigos ou partes de livro são citados com referência ao autor, título do artigo ou parte de livro, revista ou livro, volume e/ou número, ano, páginas do artigo ou parte de livro e página, quando possível. No texto, a partir da segunda citação, é apenas feita referência a autor, título do artigo ou parte de livro e página.
4. Quanto as obras ou artigos tenham sido consultados e recolhidos na Internet, a forma de citação será a seguinte: autor, título do artigo, data da publicação, hiperligação da Internet na qual foi obtido e data da consulta.
5. Nas publicações da autoria de uma instituição, o nome desta vem no lugar do autor.
6. É usado o modo itálico para destacar as palavras escritas em língua estrangeira e latinismos.
7. As transcrições de textos estrangeiros encontram-se traduzidas para português. As obras estrangeiras foram consultadas na sua língua original e a tradução é da responsabilidade da autora do presente trabalho.
8. Por uma questão de comodidade na leitura, identificam-se, ocasionalmente, as siglas ou acrónimos no texto e não apenas na secção dedicada à Lista de Abreviaturas e Siglas.
9. A presente dissertação foi redigida conforme as regras do novo Acordo Ortográfico.

Lista de Abreviaturas, Siglas e Acrónimos

AEPD	Autoridade Europeia para a Proteção de Dados
al.	alínea
AP	Administração Pública
AR	Assembleia da República
art.	artigo
arts.	artigos
CDFUE	Carta dos Direitos Fundamentais da União Europeia
Cap.	Capítulo
CEDH	Convenção Europeia dos Direitos do Homem
cfr.	conferir/conforme
DUDH	Declaração Universal dos Direitos Humanos
ELSJ	Espaço de Liberdade, Segurança e Justiça
ENISA	<i>European Union Agency for Network and Information Security</i> (Agência Europeia para a Segurança das Redes e da Informação)
JO	Jornal Oficial da União Europeia
LPD	Lei da Proteção de Dados
n.º	número
OCDE	Organização para a Cooperação e Desenvolvimento Económico
ONU	Organização das Nações Unidas

p.	página
pp.	páginas
<i>SNS</i>	<i>Social Networking Service</i> (Serviço de Rede Social)
TC	Tribunal Constitucional
TEDH	Tribunal Europeu dos Direitos do Homem
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias de Informação e Comunicação
TJ	Tribunal de Justiça
TUE	Tratado da União Europeia
UE	União Europeia
v.	<i>versus</i>
vol.	volume

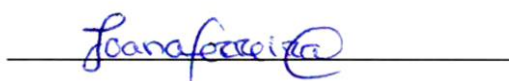
Declaração de Conformidade do Número de Caracteres

Declaro que o corpo da tese, incluindo espaços e notas, ocupa um total de 198.787 caracteres.

Declaro ainda que o Resumo utiliza 1.582 caracteres e o *Abstract* ocupa 1.538 caracteres, incluindo espaços.

Lisboa, 13 de junho de 2017

Joana Ferreira



Resumo

A evolução tecnológica e a utilização maciça da Internet colocam graves problemas quanto à proteção dos dados pessoais das pessoas. Assim, urge delimitar e entender o direito à proteção de dados pessoais, distinguindo-o do tradicional direito à privacidade e definindo-o de acordo com as fontes jurídicas de Direito Internacional, Direito da União Europeia e Direito nacional. A evolução do direito à proteção de dados no Direito da União Europeia foi progressiva e merece algum destaque e estudo, para que melhor se compreenda o atual enquadramento do regime de proteção de dados pessoais. O principal foco desta análise prende-se com o contexto europeu, uma vez que, em 2018, entrará em vigor um Regulamento Geral da União Europeia sobre a proteção de dados pessoais, o qual terá efeito direto nos Estados-Membros. A investigação é efetuada de uma perspetiva de Direitos Fundamentais, na qual se deverá concretizar a natureza do direito à proteção de dados como verdadeiro Direito Fundamental. Neste âmbito, são suscitadas diversas questões e problemas, as quais são abordadas de modo diferente, por diversos setores da doutrina. Da mesma forma, é analisada alguma jurisprudência dos Tribunais europeus e a relevante legislação. Existindo uma condição legitimante de um tratamento de dados pessoais, devem respeitar-se todos os princípios gerais orientadores destas operações. Deve, então, analisar-se o conteúdo do direito à proteção de dados, que engloba, em geral, diversas posições jurídicas como direitos dos titulares dos dados e deveres para os responsáveis pelo tratamento.

Palavras-chave: proteção de dados pessoais, direitos fundamentais, Direito da União Europeia.

Abstract

Technological developments and massive use of the Internet pose serious problems for the protection of people personal data. It is therefore necessary to delimitate and understand the right to protection of personal data, distinguishing it from the traditional right to *privacy* and defining it according to the legal sources of International Law, European Union Law and National Law. The evolution of the right to data protection in European Union Law has been progressive and deserves some emphasis and study, to better understand the current framework of the protection regime of personal data. The main focus of this analysis is the European context, since in 2018 the General Data Protection Regulation of the European Union will come into force, which will have a direct effect in the Member States. This investigation is enacted from a Fundamental Rights perspective, in which the nature of the right to data protection as a true Fundamental Right should be concretized. In this context, several questions and problems are raised, which are differently approached, by assorted sectors of the doctrine. Likewise, some case-law of the European Courts and the relevant legislation are analyzed. If there is a legitimate condition for a processing of personal data, the general guiding principles of these operations must be respected. The content of the right to data protection should therefore be examined, and encompasses, in general, several legal positions such as rights of the data subjects and obligations for data controllers.

Keywords: personal data protection, fundamental rights, European Union Law.

1. INTRODUÇÃO

A presente dissertação tem como objeto de estudo as regras de direito à proteção de dados a nível da União Europeia, não se limitando, contudo, à análise das fontes europeias.

Com o objetivo de responder à pergunta de partida “São os direitos à proteção de dados encarados como verdadeiros direitos fundamentais?”, no que diz respeito a objetivos específicos, esta dissertação visa problematizar a relação entre *Internet* e Direito e as consequências da evolução tecnológica a nível legal, refletir sobre o impacto do Novo Regulamento Geral de Proteção de Dados Pessoais no Direito da UE e no direito nacional dos Estados-Membros e salientar a importância de encarar o direito à proteção de dados como um verdadeiro direito fundamental.

O presente estudo não contém um ensaio histórico exaustivo sobre proteção de dados no Direito da UE. Apenas se distinguem as diferentes fases da evolução deste direito nos contextos internacional, europeu e nacional. Dedicar-se uma breve análise ao caso específico português, o qual merece, também, referências ao longo de cada um dos capítulos.

Atualmente, se, por exemplo, assistirmos a uma palestra e nos for referido o nome de um Autor, do qual nunca ouvimos falar, basta-nos efetuar uma simples pesquisa *online*, a qual se pode realizar num período inferior a cinco minutos, e, desta forma, obtemos informações que podem referir-se ao nome, data de nascimento, profissão, obras publicadas, biografia pessoal e outros dados relativos a essa pessoa. Assim, acedemos, facilmente, a inúmeros dados pessoais de qualquer pessoa pela qual pesquisemos. Mas, e se não quisermos os nossos dados pessoais disponíveis a terceiros? Que direitos nos são conferidos para que possamos controlar os dados que nos dizem respeito?

Esta dissertação tem como objeto o estudo das posições jurídicas relativas à proteção de dados pessoais, a nível da UE, as quais são pertinentes de investigar, dada a sua atualidade e a adoção do novo Regulamento da UE, o qual será diretamente aplicável nos seus Estados-Membros.

Assim, importa explicitar a estrutura da presente dissertação. Após o 1.º Capítulo, o qual concerne à Introdução, no 2.º Capítulo, será explicitada a relação entre as novas tecnologias, em particular a *Internet*, e o Direito, de modo a definir que este não pode nem deve subtrair-se do mundo digital. Neste ponto, elucida-se sobre as dificuldades práticas da privacidade neste meio da *Internet*.

Seguidamente, no 3.º Capítulo, são referidas as principais fontes jurídicas do direito à proteção de dados e as quais inspiraram, também, o novo Regulamento Geral, designadamente as de origem internacional, europeias e nacionais.

Após esta breve análise, torna-se necessário, no 4.º Capítulo, proceder a um enquadramento do conceito de direito à proteção de dados, a partir da definição dos conceitos primordiais desta temática, nos quais se incluem a própria expressão “dados pessoais”, e as suas respetivas categorias, e “tratamento de dados pessoais”. Neste Capítulo distinguem-se os direitos à privacidade e à proteção de dados, apresentando-se as relevantes doutrinas existentes a este propósito.

Deste modo, procede-se, finalmente, à análise, sediada no 5.º Capítulo, do direito à proteção de dados pessoais, no âmbito do novo Regulamento, de uma perspetiva de Direitos Fundamentais. Assim, parte-se de uma breve história da evolução deste direito, e consideram-se, então, os princípios orientadores do tratamento de dados pessoais, os direitos conferidos aos titulares dos dados e os deveres impostos aos responsáveis por este tratamento.

Deve, ainda, deslindar-se, relativamente ao tema tratado em cada um dos capítulos, o modo de resolver as questões relacionadas com a aplicação deste direito no âmbito da *Internet*.

Existem diversos meios nos quais ao direito à proteção de dados é conferida importância reforçada, como é o caso dos meios de comunicação, os modos de videovigilância, entre outros. Porém, por motivos de delimitação temática, para efeitos da presente dissertação, apenas será considerado o meio digital da *Internet*.

Deve especificar-se que os termos de “*Internet*”, “ciberespaço” ou “rede aberta” são utilizados, no presente estudo, enquanto sinónimos, pretendendo, sempre, significar a *Internet* enquanto uma rede aberta de comunicação através de computadores.

A perspetiva na qual se analisa o contexto deste direito é, exclusivamente, legal. Não se abordam com profundidade as questões mais técnicas desta temática, as quais mereceriam uma devida consideração, mas a qual não cabe no âmbito do presente estudo.

Importa referir que as fontes utilizadas para o estudo das questões levantadas ao longo da dissertação são fontes de acesso público, as quais incluem obras monográficas e coletivas, artigos científicos, legislação e jurisprudência europeia.

Ao longo do texto, serão utilizados alguns termos específicos da temática em análise, os quais devem ser aludidos com rigor terminológico e, por esse motivo, a sua referência é realizada na língua original. Porém, nos restantes casos, nos quais é possível efetuar uma tradução o mais fiel possível, a mesma é feita, sob responsabilidade da Autora, como forma de tornar a leitura mais simples e aprazível.

Porventura, seria conveniente uma abordagem de Direito Comparado sobre certos aspetos da evolução do direito à proteção de dados, porém não será incluída essa análise, sendo, contudo, referidos alguns casos nacionais específicos que se revestem de particular singularidade relativamente a determinadas questões.

A presente dissertação não pretende esgotar, através de uma análise exaustiva, o estudo do direito à proteção de dados a nível internacional, europeu ou português. O objetivo é, pois, expor as questões consideradas mais relevantes neste âmbito e demonstrar o “estado da arte” com a adoção do novíssimo Regulamento Geral de Proteção de Dados.

Trata-se, assim, de apresentar a dogmática do direito à proteção de dados pessoais no Direito da União Europeia, no contexto da Sociedade da Informação, na qual a tecnologia de informação e a *Internet* se encontram intimamente conectadas e levantam diversos problemas jurídicos.

A abordagem na qual se estuda o presente tema é realizada, primordialmente, à luz dos Direitos Humanos ou Direitos Fundamentais, não se abordando questões civis ou criminais. Da mesma forma, não se aprofundam assuntos relativos à teoria geral dos Direitos Fundamentais.

Assim, devem estudar-se as novas regras europeias sobre o direito à proteção de dados e conhecer as distintas teorias doutrinárias respeitantes a este direito e a questões com este interligadas.

2. RELAÇÃO ENTRE O CIBERESPAÇO E O DIREITO

Não se deve passar imediatamente para a análise de aspetos jurídicos sobre a rede mundial sem explicar antes o papel natural e necessário de regulação e otimização dos interesses dos sujeitos que o Direito tem neste espaço *online*. O ciberespaço é um mundo onde confluem inúmeras informações, é uma dimensão onde não existe tempo nem espaço, mas na qual é necessária uma apertada regulação jurídica, nomeadamente no que toca aos direitos das pessoas. Entre esses direitos releva o direito à privacidade.

2.1. Evolução Tecnológica e modelos de regulação jurídica do ciberespaço

A *Internet* (*Inter Communication Network*) é uma rede internacional de computadores que comunicam entre si através de uma linguagem informática, o *Transport Control Protocol/Internet Protocol* (TCP/IP), enviando pacotes de informação de que fazem parte os endereços IP do remetente e do destinatário.¹

A *Internet* começou por ser, na figura da sua antecessora (a *ARPANet*), um instrumento da Guerra Fria, criada pela *Defense Advanced Research Projects Agency* (*DARPA*) em 1969, para ligar departamentos de investigação e investigadores à *DARPA*.² Com o passar do tempo, foi-se assistindo a uma globalização da rede, deixando de ser uma rede privada, para passar a ser uma rede acessível a toda e qualquer pessoa em todo o Mundo.

Como evidencia José de Oliveira Ascensão, a *Internet* “permitiu a experimentação de um tipo de comunicação de âmbito mundial.”³

¹ CASTRO, Catarina Sarmiento - Direito da Informática, Privacidade e Dados Pessoais. Coimbra: Almedina, 2005, pp. 153-154.

² *Idem*, Protecção de dados pessoais na *Internet*. **Sub Judice. Justiça e Sociedade**. n.º 35, Set. 2006, pp. 11-22. P. 13.

³ ASCENSÃO, José de Oliveira - Estudos sobre direito da *Internet* e da sociedade da informação. Coimbra: Almedina, 2001, p. 85.

Atualmente, assistimos a um fenómeno de disseminação das novas tecnologias e de uso maciço da *Internet*, a todos os níveis, tais como o profissional, o pessoal e o escolar. Realça-se o papel da *Internet* como modo de acessibilidade da informação através de redes mundiais de comunicação eletrónicas. Com o intercâmbio global de informação através da rede torna-se ainda mais visível o fenómeno da globalização.

Mas em que consiste a “informação”? Na esteira de Dário Moura Vicente, por “informação” deve entender-se os dados ou conteúdos que podem ser objeto do conhecimento humano.⁴ Assim sendo, encontramos-nos numa verdadeira Sociedade da Informação.⁵

O rápido desenvolvimento das TIC, determinado por um fenómeno como a *Internet*, facilitou a evolução para uma sociedade global de informação.

Na Sociedade da Informação, a *Internet* é indispensável para grande parte das tarefas diárias. De manhã, acedemos ao nosso correio eletrónico, à tarde, no emprego, trabalhamos através de um computador, utilizando diversas plataformas eletrónicas, e à noite visitamos as nossas redes sociais. Todas estas atividades utilizam informações ou dados pessoais.

Porém, apesar de todos os benefícios e desenvolvimento económico, social e cultural que adveio com este fenómeno tecnológico, o mesmo não é isento de perigos, muitos deles gravíssimos e que violam, flagrantemente, a dignidade humana. Exemplos disso são os casos de cibercrime, isto é, crimes cometidos através da rede. Através da *Internet*, são, também, cometidos crimes de terrorismo, de pornografia infantil, de *cyberbullying*, de incitamento à violência e ao ódio, de tráfico de estupefacientes, de roubo de dados e identidade, de difamação e injúrias, entre outros.

Os problemas jurídicos suscitados pela Sociedade da Informação são de várias ordens: como exemplifica Dário Moura Vicente, tornou-se necessária a

⁴ VICENTE, Dário Moura - Direito Internacional Privado: Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, p. 13.

⁵ Ou Sociedade da Comunicação, como explica ASCENSÃO, José de Oliveira, *Op. cit.*, 2001, p. 87.

institucionalização de meios de controlo do uso da informática (nomeadamente, para tutelar a privacidade das pessoas), surgiram novas categorias de bens intelectuais e novos meios de transmissão, utilização e exploração da informação, assistiu-se a uma expansão das redes públicas de comunicações eletrónicas (a qual estimulou o comércio eletrónico), passou a estar disponível em rede informação ilícita e impôs-se a questão de saber como pode a tecnologia determinar a solução de conflitos de interesses.⁶

Deste modo, é indispensável um modelo de regulação jurídica do ciberespaço, não podendo estes crimes passar impunes apenas por se realizarem num meio desmaterializado e digital. Mas, tal como afirma Jorge Bacelar Gouveia, o Direito cedo se tornou sensível a esta problemática e a disciplina jurídica foi-se dilatando por diversos ramos jurídicos, sendo o mais relevante o que diz respeito às preocupações do Direito Constitucional.⁷

De acordo com Mayer-Schönberger, há três modelos possíveis para a “governança da *Internet*”: o modelo tradicionalista, no qual se estabelece uma analogia com a governação estatal, o modelo ciber-separatista, segundo o qual a *Internet* seria um espaço alargado de liberdade, isento de regulação e fronteiras, e o modelo internacionalista, através do qual se permitiria a instrumentos de Direito Internacional a regulação deste espaço, para que à globalização da rede correspondesse a unidade na regulação. A proposta deste autor baseia-se em tópicos de decisão que articulem os três paradigmas, de forma casuística.⁸

⁶ VICENTE, Dário Moura, 2005, *op. cit.*, pp. 14-15.

⁷ GOUVEIA, Jorge Bacelar - Os Direitos Fundamentais à Protecção dos Dados Pessoais Informatizados. In: **Revista da Ordem dos Advogados**, Ano 51-III, 1991, pp. 700-732. Pp. 700-701.

⁸ MAYER-SCHÖNBERGER, Viktor - *The shape of governance. Analyzing the world of Internet regulation*, Va. J. Int'l L, vol. 43, 2003, p. 612. *Apud* PINHEIRO, Alexandre Sousa - *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*. Lisboa: AAFDL Ed., 2015. Pp. 227-230.

Ora, se uma hiper-regulação da *Internet*, ao restringir o fluxo transfronteiriço da informação e o seu acesso público, pode prejudicar a liberdade na qual assenta a Sociedade da Informação, também não deve ser aceitável uma total inexistência de normas reguladoras deste espaço virtual.⁹ Isto porque o “virtual” não deixa de ser um espaço de comunicação humana que não se exime à necessidade de respeitar o princípio da dignidade humana, não sendo, por isso, compatível com comportamentos degradantes, humilhantes ou de outra natureza.¹⁰

Uma regulação jurídica do espaço digital não compromete, de forma alguma, o ideal de liberdade almejado através da *Internet*. Este objetivo de liberdade deve sempre ser harmonizado com o exercício das soberanias nacionais, concluindo-se, assim, que o problema assenta, não na inexistência de lei aplicável, mas sim no facto de surgirem diversas leis nacionais potencialmente aplicáveis.¹¹

Desta forma, apesar de a *Internet* ser encarada como um espaço livre de direito e de regulação, sendo um veículo privilegiado para o exercício das liberdades, está sujeita a regras que pretendem regular a sua utilização¹².

De todos os problemas jurídicos suscitados pela utilização da *Internet*, assinalamos os relativos à proteção da privacidade e dos dados pessoais. Ora, o uso da *Internet* leva a que, tanto operadores de telecomunicações, como fornecedores de acesso à *Internet*, e até titulares dos sítios *online*, recolham e tratem dados pessoais dos utilizadores dos seus serviços. Se a informação pessoal circula sem fronteiras na *Internet*, a divulgação e recolha destes dados pessoais deve estar sujeita a regulamentação. Não é por a divulgação se realizar no mundo digital que a pessoa perde os seus direitos e liberdades fundamentais.

⁹ VICENTE, Dário Moura, 2005, *op. cit.*, p. 96.

¹⁰ PINHEIRO, Alexandre Sousa, 2015, *op. cit.*, p. 230.

¹¹ Para um estudo detalhado sobre estas questões de Direito Internacional Privado e de avaliação dos métodos de regulação deste espaço, consultar VICENTE, Dário Moura, 2005, *op. cit.*.

¹² CASTRO, Catarina Sarmento – *Op. cit.*, 2006, p. 11.

Através da *Internet*, a divulgação de informações pessoais é instantânea e feita a uma escala global, traduzindo-se numa compressão da privacidade das pessoas. A maior partilha de dados pessoais de todos os tempos e a dimensão global e irreversível dessa partilha na rede levanta problemas graves na proteção desses dados.

Assim, ao nível da proteção de dados pessoais na *Internet*, algumas das questões geradas dizem respeito aos *cookies*, ao acesso generalizado a redes sociais, à distribuição da informação em sistemas de nuvem, à comunicação por correio eletrónico e aos direitos fundamentais incluídos nesta proteção.

Para uma proteção de dados pessoais efetiva, a legislação atual deve ser atualizada e adaptada às novas tecnologias e ao facto de ser o próprio utilizador a disponibilizar a informação a si respeitante. Assim, o titular deve controlar os seus próprios dados pessoais.

Em conclusão, não só o Direito está presente no ciberespaço pelo facto de neste se levantarem várias questões jurídicas, como diversos autores defendem a existência de um novo ramo do Direito direcionado para a Informática, denominado Direito da Sociedade da Informação ou Direito da Informática, o qual disciplina os problemas suscitados pela produção, transmissão e utilização deste bem imaterial na base de uma específica ponderação dos valores/interesses em jogo.¹³

Deste modo, deve analisar-se a problemática dos direitos de personalidade, concretamente, o direito à privacidade, perante o tratamento de dados pessoais na Sociedade da Informação.

2.2. A Privacidade é um mito na *Internet*?

As TIC e a *Internet* revolucionaram a sociedade e o modo de vida das pessoas. As pessoas comunicam através da *Internet*, o fornecimento de bens e de serviços realiza-se digitalmente, as Administrações Públicas disponibilizam serviços pelo seu sítio na *Internet* e, nas empresas, o trabalho concretiza-se informaticamente.

¹³ VICENTE, Dário Moura, 2005, *op. cit.*, p. 16.

Através de processamento automático, a Informática cria, comunica e trata dados.

Com esta maior utilização da *Internet* e dos seus recursos, também o volume de informações pessoais recolhidas e tratadas na rede aumentou exponencialmente. Estas informações são, por vezes, recolhidas sem o consentimento do seu titular, o que põe em causa a privacidade das pessoas.

As novas possibilidades de armazenamento na rede de quantidades maçicas de informações pessoais e de fácil acessibilidade potenciam os problemas colocados pela denominada “*digital eternity*”, isto é, a “eternidade digital”. Enquanto no mundo físico, certas situações da vida seriam facilmente esquecidas pela memória efémera do ser humano com o passar do tempo, no mundo virtual, as informações que foram disponibilizadas ou partilhadas pelo próprio titular das mesmas ou por terceiros podem ter um carácter de permanência irreversível na memória perene do ciberespaço. Isto porque estas informações têm tendência a ser lembradas pela memória digital, podendo, até mesmo, ter sido recolhidas por outrem.

As informações publicadas num certo contexto informal podem ser acedidas e utilizadas noutros contextos para formar julgamentos em detrimento desse indivíduo, ou seja, a *Internet* potencia o problema da “descontextualização”.¹⁴

Esta descontextualização pode distorcer informações sobre o indivíduo à qual respeitam e, uma vez que a *Internet* não esquece, é importante existir uma regulação jurídica segura para este tipo de situações.

Numa sociedade de recolha e partilha massiva de dados, a utilização da *Internet* deve ser conciliada com o direito das pessoas à privacidade e, assim, impõe-se a questão de saber o significado da privacidade, o qual tem variado ao longo dos tempos. Porém, como recorda Giovanni Buttarelli, não se deve nunca descurar que a sociedade é construída a partir de valores humanos, os quais devem sempre ser

¹⁴ LINDSAY, David - The «right to be forgotten» in European data protection law. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 290–337. Pp. 294–295

respeitados de modo a que a ética e a inovação se interliguem harmonizadamente e se mitiguem as tensões existentes entre ambos.¹⁵

Podemos considerar a “privacidade” como o direito à intimidade e à reserva de informações pessoais e da vida privada e familiar, englobando, também, o direito de controlar os dados que nos dizem respeito e a sua disponibilidade perante os outros, seja ao nível da *Internet*, como a todos os restantes meios de divulgação e partilha dos mesmos. Este conceito tem vindo a ser reformulado devido às evoluções sociais e tecnológicas, uma vez que se tornou muito mais fácil concretizar uma utilização abusiva das informações pessoais que atente contra os direitos, liberdades e garantias das pessoas, concretamente, o direito à privacidade ou à reserva da intimidade da vida privada e familiar, como consagrados pela CRP, no art. 26.º.

Hoje em dia, é possível saber-se as preferências do indivíduo, os seus locais visitados, os seus interesses e diversas outras informações através da *Internet* e, nomeadamente, através das redes sociais.

Aliás, visto que a recolha e partilha de dados pessoais pode acarretar graves consequências para a privacidade das pessoas e pode violar outros princípios fundamentais (tais como o da autodeterminação informacional e o do direito de acesso aos dados pelo seu titular), devem ser adotadas novas configurações jurídicas que respondam, de forma efetiva, aos problemas colocados pela Sociedade da Informação. E, assim, o objetivo passará sempre por garantir o controlo dos dados pelos seus titulares. Este direito à privacidade pode, também, entrar em conflito com diversas liberdades, tais como a liberdade de informação e comunicação e a liberdade de expressão.

São inúmeros os desafios relativos à privacidade que se colocam neste meio: o consentimento dos titulares dos dados, o controlo dos dados pessoais pelo seu titular, a preservação da privacidade através de técnicas de anonimização e a regulação por meio de mecanismos que assegurem um nível adequado de

¹⁵ BUTTARELLI, Giovanni - Ethics at the Root of Privacy and as the Future of Data Protection. 2016, p. 4.

proteção.¹⁶

Como conclui Alexandre Sousa Pinheiro, “Em suma, o clima sociocultural em que vivemos não favorece a *privacy*, nem a proteção de dados. Estranha-as.”¹⁷.

Para se proteger a privacidade no mundo virtual deve assegurar-se uma regulamentação mais eficaz, através de uma disciplina do uso da *Internet* e de uma cooperação entre os países, por meio de sanções mais gravosas para os casos de não cumprimento das regras, pelo uso da própria tecnologia de modo a proteger os dados dos utilizadores e pela consciencialização do próprio titular de dados relativamente aos problemas da publicação e partilha das suas informações na *Internet*.

A proteção da privacidade dos titulares dos dados começa com a sua atuação na rede, ao nível da colocação e partilha dos seus dados pessoais na *Internet* e na sua consciencialização sobre os perigos e riscos do ciberespaço.

Assim, na esteira de Catarina Sarmiento e Castro, “Da consciência, da sensibilidade, da informação e dos conhecimentos de que dispõe o utilizador dependem em grande medida as garantias que saberá fazer funcionar a favor da sua privacidade.”¹⁸

A privacidade é protegida independentemente do carácter informático do instrumento de agressão. Assim, a privacidade existe, sim, na *Internet*, mas está sujeita a riscos cada vez maiores com a evolução deste mundo digital e deve, por isso, adotar-se uma regulamentação segura e eficiente.

¹⁶ ANTUNES, Luís Filipe - A privacidade no mundo conectado da *Internet* das coisas. In: **Fórum de Protecção de Dados**, n.º 2, pp. 52–58. Lisboa, 2016. P. 56

¹⁷ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 107

¹⁸ CASTRO, Catarina Sarmiento, 2005, *op. cit.*, p. 156.

3. FONTES JURÍDICAS DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

O tráfico jurídico internacional de informação entre computadores tem-se intensificado, sobretudo nos últimos anos. Para proteger a vida privada perante as ameaças impostas pelos meios informáticos e tecnológicos cada vez mais avançados de recolha e tratamento de informações pessoais, o Direito tem de regular estas matérias, nomeadamente, no que toca ao mundo virtual.

Os dados pessoais não encontram fronteiras, mas as leis sobre a proteção de dados e sobre a privacidade tiveram origem, primordialmente, nas ordens jurídicas dos Estados. Todas estas regras têm como um dos seus principais objetivos a proteção do titular dos dados. Neste sentido, analisam-se as fontes jurídicas das regras que respeitam ao tratamento dos dados pessoais, para depois proceder à delimitação do sentido e do termo “dados pessoais” e outras noções relevantes, de acordo com os instrumentos jurídicos mais relevantes na temática em estudo.

Afigura-se necessário proceder a três considerações iniciais para que se prossiga com o presente estudo.

Em primeiro lugar, deve explicitar-se que a perspetiva na qual são utilizadas as expressões “Direitos Fundamentais” ou “Direitos Humanos” mais não é do que no sentido de que *“enquanto os direitos humanos são direitos de todos os indivíduos, tenham ou não a nacionalidade de um determinado país, os direitos dos cidadãos são direitos fundamentais que são exclusivamente garantidos aos nacionais de um determinado país (...).”*¹⁹

Assim, é seguida uma distinção baseada num critério de fonte, segundo a qual os direitos fundamentais são encontrados, de forma geral, nos textos constitucionais,

¹⁹ BENEDEK, Wolfgang (ed.) - Understanding Human Rights Manual on Human Rights Education. Viena: European Training and Research Centre for Human Rights and Democracy, 3.^a ed., 2012. P. 39.

enquanto os direitos humanos se referem às garantias fundamentais integrantes do Direito internacional.²⁰

Em segundo lugar, consideramos que os “Direitos Fundamentais” são os pressupostos elementares e básicos da vida humana livre e digna, constituindo direitos essenciais e principais que caracterizam a pessoa e se ligam com a dignidade da pessoa humana.²¹

Por último, importa esclarecer que se preferiu utilizar a expressão “Direitos Humanos” e não “Direitos do Homem”, que, além de acompanhar melhor a tradução da expressão generalizada a nível internacional de “*Human Rights*”, garante uma perspectiva neutra no género. Seguimos, assim, a recomendação encetada pela Assembleia da República (AR), na Resolução n.º 39/2013, de 3 de abril de 2013²², na qual a AR apela ao Governo e às entidades públicas e privadas para que adotem a expressão universalista.²³

Importa precisar que a análise que ora se concretiza, em cada subcapítulo, de cada uma das fontes jurídicas reguladoras da proteção de dados, inclui considerações relativas à categorização do direito à proteção de dados pessoais como Direito Fundamental (ou Direito Humano, consoante a fonte, tal como explicitado), de modo a conduzir a um mais profundo comentário sobre esta classificação em capítulo ulterior.

²⁰ OLIVEIRA, Bárbara Nazareth, GOMES, Carla de Marcelino e SANTOS, Rita Páscoa dos - Os Direitos Fundamentais em Timor-Leste: Teoria e Prática. Coimbra: *Ius Gentium Conimbrigae* — Centro de Direitos Humanos da Faculdade de Direito da Universidade de Coimbra, 2015. P. 31.

²¹ ANDRADE, José Carlos Vieira de – Os Direitos Fundamentais na Constituição Portuguesa de 1976. Coimbra: Almedina, 4.ª ed., 2009. Pp.92-108.

²² Resolução da Assembleia da República n.º 39/2013, de 3 de abril de 2013. Publicada no Diário da República n.º 65/2013, Série I de 2013-04-03, p. 1950.

²³ A utilização da expressão “Direitos do Homem” em Portugal radica, sobretudo, na tradução portuguesa da CEDH de 1950, firmada no seio do Conselho da Europa, na qual se partiu da versão francófona que utiliza o termo “*droits de l’homme*”, que, apesar do seu valor histórico, urge rever face aos desenvolvimentos de Direito Internacional.

Por conseguinte, primeiro serão analisadas as fontes de Direito Internacional, nas quais se incluem as regras adotadas pela ONU, pela OCDE e pelo Conselho da Europa. Depois, passaremos ao tratamento das fontes jurídicas de Direito da União Europeia (UE), o que abarca Tratados, Diretivas e Regulamentos, mas também outros instrumentos relevantes, nomeadamente Resoluções, Recomendações e Comunicações. Por fim, examinam-se as mais expressivas fontes de Direito Nacional, concretamente a Constituição da República Portuguesa (CRP) e a legislação específica sobre a matéria.

3.1. Fontes de Direito Internacional

A globalização depende, em larga medida, da *Internet* e da conectividade que, por sua vez, implica um intenso fluxo transfronteiriço de dados pessoais.

A partir de 1980, começaram a ser adotados, por diversas organizações internacionais, instrumentos internacionais sobre o tratamento de dados e, por conseguinte, disseminaram-se pelo Mundo as normas reguladoras desta matéria.

Neste sentido, foram adotados dois instrumentos-chave internacionais: em 1980, as Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais e, em 1981, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, comumente designada por Convenção n.º 108, do Conselho da Europa.

Assim, serão analisados, de forma breve, os mais importantes instrumentos reguladores desta temática a nível de Direito Internacional, pela parte da Organização das Nações Unidas (ONU), da Organização para a Cooperação e Desenvolvimento Económico (OCDE) e do Conselho da Europa.

3.1.1. Organização das Nações Unidas (ONU)

A Organização das Nações Unidas (ONU) manifesta, desde cedo, interesse na área da proteção de dados pessoais e da privacidade, organizando ações e conferências relativas a esta temática, nomeadamente a anual “*International Conference of Data Protection and Privacy Commissioners*”, a qual tem lugar desde 1979 e conta com a

presença de 115 autoridades de proteção de dados e da privacidade de todo o Mundo²⁴. Estas Conferências envolvem, desde 2003, a adoção final de uma Resolução, sobre variadas questões relacionadas com estas temáticas.

A ONU elabora, ainda, relatórios na sequência de estudos encetados relativamente a estes assuntos, como o Relatório denominado “O Direito à Privacidade na Idade Digital”, de 2014, do Alto Comissariado das Nações Unidas para os Direitos Humanos²⁵.

3.1.1.1. Declaração Universal dos Direitos Humanos e Pactos

A Declaração Universal dos Direitos Humanos (DUDH), proclamada em 1948, consagra, no artigo 12.º o direito à privacidade, mas não define esta noção.

Também o Pacto Internacional dos Direitos Civis e Políticos, de 1966, consagra um direito à privacidade, no art. 17.º, que é muito semelhante ao contido na DUDH.

3.1.1.2. Diretrizes Para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal

Apenas em 1990, a Assembleia Geral das Nações Unidas adotou, através da Resolução n.º 45/95, as Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal. Estas Diretrizes englobam princípios relativos às garantias mínimas que devem ser consagradas na legislação nacional e regras sobre a aplicação das diretrizes aos ficheiros de dados de carácter pessoal mantidos por organizações internacionais de carácter intergovernamental.

3.1.1.3. Direito à proteção de dados pessoais como Direito Humano no âmbito da ONU

Apesar de a ONU não se referir, na DUDH, ao direito de proteção de dados pessoais, deve ter-se em conta que este direito apenas adquiriu autonomia com o advento das novas tecnologias e com o tratamento maciço de dados pessoais e que

²⁴ Para mais informações: <https://icdppc.org/>.

²⁵ Resolução n.º 68/167, de 18 de dezembro de 2013. Documento A/RES/68/167.

é, por isso, natural a ausência de referências a este direito. Com o passar do tempo, a ONU tem-se debruçado sobre esta questão e tem referido, gradualmente, a proteção de dados.

Na Resolução n.º 68/167, a Assembleia Geral solicitou ao Alto Comissariado das Nações Unidas para os Direitos Humanos a apresentação de um relatório sobre a proteção e promoção do direito à privacidade no contexto da vigilância doméstica e extraterritorial e da interceção de comunicações digitais e da recolha de dados pessoais. Na referida Resolução reafirma-se o direito humano à privacidade e reconhece-se a natureza aberta e global da *Internet*, a qual, em cumulação com os rápidos avanços nas TIC, conduz a uma aceleração do progresso e do desenvolvimento.

Portanto, apesar de sub-categorizado no direito à privacidade, o direito à proteção de dados não deixa de ser tratado com natureza de Direito Humano nos diversos instrumentos da ONU.

3.1.2. Organização para a Cooperação e Desenvolvimento Económico (OCDE)

A Organização para a Cooperação e Desenvolvimento Económico (OCDE) tem promovido uma iniciativa, denominada “Novas Fontes de Crescimento: o Capital Baseado no Conhecimento”, com o fim de promover a inovação e a confiança numa economia orientada por dados.²⁶

Para além deste projeto, tem adotado diversos instrumentos relevantes para a regulação da proteção de dados.

3.1.2.1. Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais

Tal como referido, foram adotados dois instrumentos-chave internacionais na matéria da proteção dos dados pessoais. O primeiro foi adotado em 1980, e diz respeito às Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos

²⁶ BUTTARELLI, Giovanni - Value of the EU Data Protection Reform against the Big Data challenges. 5th European Data Protection Days, Berlim, 2015. P. 4

Transfronteiriços de Dados Pessoais²⁷, as quais, apesar de não serem legalmente vinculativas, representam o consenso internacional no que diz respeito à recolha e tratamento de informação pessoal e foram adotadas por comum acordo entre os Estados Unidos da América (EUA) e os países europeus.

As Diretrizes da OCDE tiveram como objetivo equilibrar a proteção da privacidade com o objetivo de um “fluxo livre” transfronteiriço de dados pessoais.

3.1.2.2. Direito à proteção de dados pessoais como Direito Humano no âmbito da OCDE

Apesar de considerar o direito à privacidade e o direito à proteção de dados, muitas vezes, como intrinsecamente ligados, não adquirindo autonomia por si só, a OCDE procedeu à adoção de diversos instrumentos com vista a protegê-los, nomeadamente no que concerne ao perigo da sua violação com o advento das novas tecnologias, tratando-os como Direitos Humanos.

3.1.3. Conselho da Europa

Os principais instrumentos de Direito Internacional relativos a Direitos Humanos não fazem referência expressa à proteção dos dados pessoais, optando pela proteção da privacidade ou da vida privada, veja-se os referidos casos da DUDH, da ONU, e da própria Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais, do Conselho da Europa.

Apenas nos anos 70, o Conselho da Europa reestruturou o seu interesse no problema da proteção das pessoas face aos desenvolvimentos tecnológicos, entendendo-o como um problema de privacidade, com necessidade de regulação.

²⁷

Disponível

em

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm> (24/02/2017). Entretanto, em 2013, estas Diretrizes da OCDE foram atualizadas e adaptadas a novos problemas que surgiram ao longo dos últimos 30 anos. Para mais informações, consultar <https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm> (24/02/2017).

3.1.3.1. Convenção Europeia dos Direitos do Homem (CEDH) e
Jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH)

A Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais ou Convenção Europeia dos Direitos do Homem (CEDH), de 1950, tornou-se o mais importante instrumento de Direitos Humanos a nível europeu e, como tal, deve analisar-se o seu art. 8.º.

O art. 8.º, epigrafado como “Direito ao respeito pela vida privada e familiar”, apresenta a seguinte formulação:

“1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.”

Como se verifica, este artigo não refere a privacidade, mas sim o “respeito da vida privada e familiar”. De acordo com Gloria Fuster²⁸, este facto pode ser explicado, presumivelmente, tendo em conta a influência da expressão francesa, uma vez que os esboços originais incluíam “privacidade”, mas foram alterados para que se mantivesse a consistência com a versão original francesa do artigo 12.º da DUDH, na qual apenas se refere a “vida privada”, contrariamente à versão inglesa, que alude especificamente a “privacidade”.²⁹

Contudo, a “*privacy*”, em inglês, e a “*vie privée*”, em francês, têm sido considerados como equivalentes em diversos instrumentos internacionais.

Apesar de a jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH)

²⁸ FUSTER, Gloria González - The Emergence of Personal Data Protection as a Fundamental Right of the EU. Londres: Springer Ed.. P. 82

²⁹ Cfr. a versão inglesa: <http://www.un.org/en/universal-declaration-human-rights/> e a versão francesa: <http://www.un.org/fr/universal-declaration-human-rights/> (06/06/2017).

ter alargado o entendimento da noção constante do art. 8.º da CEDH ao longo dos anos, foi defendido, nos anos 70, que, com o advento informático, o supramencionado artigo não oferecia a devida proteção às pessoas.³⁰

No caso *Gaskin*, de 1989, o TEDH encarou a recusa, pela AP, de acesso dos indivíduos à sua informação armazenada como uma ingerência nos direitos do art. 8.º.³¹

O TEDH, com o objetivo de proteção da privacidade, tem entendido o art. 8.º da CEDH com um sentido amplo e, na ausência de uma disposição mais específica, este também é relevante para a proteção de dados.

Os direitos consagrados na CEDH influenciam, fortemente, o Direito da UE, uma vez que esta Convenção é vinculativa para os seus Estados-Membros. Assim, os seus direitos incorporam os princípios gerais de Direito da UE, tal como estabelecido no n.º 3 do art. 6.º do TUE, e a própria União está em processo de adesão à CEDH³², conforme estabelecido no n.º 2 do mesmo artigo.

3.1.3.2. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal

O segundo instrumento-chave internacional no que toca ao direito à proteção de dados é a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal³³, de 1981, a Convenção n.º 108, que constituiu o primeiro instrumento internacional vinculativo quanto à proteção das pessoas no que diz respeito a abusos que possam ter lugar no momento da recolha e

³⁰ FUSTER, Gloria González – *Op. cit.*, 2014. Pp. 94-95.

³¹ Caso *Gaskin v. The United Kingdom*, de 7 de julho de 1989, n.º 12 EHRR 36.

³² WITZLEB, Normann, LINDSAY, David, PATERSON, Moira e RODRICK, Sharon – An overview of emerging challenges in privacy law. **Emerging challenges in privacy law: comparative perspectives**, pp. 1-28. Cambridge: Cambridge University Press, 2014. P. 10.

³³ Disponível em <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> (24/02/2017).

tratamento de dados pessoais, regulando, simultaneamente, o fluxo transfronteiriço de dados pessoais.

A Convenção n.º 108 contém regras de proteção de dados, com o fim de assegurar direitos e liberdades, particularmente, o direito à privacidade. Podemos assumir que o direito à privacidade prosseguido pelas regras de proteção de dados corresponde ao direito ao respeito da vida privada consagrado no art. 8.º da CEDH.³⁴

Tanto a Convenção n.º 108 como as Diretrizes da OCDE promoveram uma evolução desta matéria e levaram o TEDH a expandir a sua interpretação do art. 8.º da CEDH, de modo a abranger a proteção das pessoas face a algumas práticas informáticas.

Quando foi adotada a Convenção n.º 108, esta foi aberta a países não europeus e levou a que os Estados Contratantes adotassem a sua própria legislação interna referente ao assunto, uma vez que a Convenção n.º 108 exige, como condição para a sua ratificação, a adoção de legislação interna que cumpra o conteúdo da Convenção pelos Estados, como definido no art. 4.º.

Esta Convenção visa assegurar, para cada pessoa, independentemente da sua nacionalidade ou residência, o respeito pelo direito à proteção de dados. O princípio da equivalência constitui o critério-chave para o fluxo transfronteiriço de dados, uma vez que, subscrevendo o núcleo comum de regras de proteção de dados, cada Estado oferece um certo nível mínimo de proteção, permitindo a circulação dos dados. Porém, ao proibir transferências para Estados Não Contratantes, a Convenção não se coloca a par das necessidades crescentes de transferências transfronteiriças.³⁵

3.1.3.3. Direito à proteção de dados pessoais como Direito Humano no âmbito do Conselho da Europa

Apesar de a CEDH apenas consagrar o direito humano à privacidade, tem sido

³⁴ FUSTER, Gloria González – *Op. cit.*, 2014. P. 104.

³⁵ KONG, Lingjie – Data Protection and Transborder Data Flow in the European and Global Context. *In: European Journal of International Law*, V. 21, *Issue* 2, 2010, pp. 441-456. P. 442.

defendido que o direito à proteção de dados adquiriu um significado autónomo ao longo dos últimos 30 anos, através de jurisprudência do TEDH e da Carta dos Direitos Fundamentais da UE (CDFUE).³⁶

Existe, ainda, quem defenda que a Convenção n.º 108 constitui o único tratado global de proteção de dados, devido ao facto de os restantes instrumentos internacionais existentes na regulação desta temática serem juridicamente não vinculativos, tal como as Diretrizes da OCDE, ou compreenderem um limitado âmbito de aplicação territorial, como é o caso das Diretivas da UE.³⁷

Além disso, o Conselho da Europa tem promovido a elaboração de orientações para os Governos em matéria de proteção de dados pessoais e tem adotado, através do Comité de Ministros, diversas Recomendações direcionadas a diversos setores da sociedade tendo em vista questões relacionadas com esta temática. Podemos considerar o direito à proteção de dados pessoais, no âmbito do Conselho da Europa, um verdadeiro Direito Humano.

Por conseguinte, a proteção de dados pessoais encontra-se diretamente ligada à proteção dos Direitos Humanos e das liberdades fundamentais, sendo um pressuposto do Estado Democrático.³⁸

3.2. Fontes de Direito da União Europeia (UE)

3.2.1. Tratados e Carta dos Direitos Fundamentais da UE

A partir dos anos 2000, a “revolução digital” tornou-se um dos objetivos primordiais da UE, sendo relevante para a qualidade de vida dos seus cidadãos, para

³⁶ A questão da distinção entre privacidade e proteção de dados será abordada, mais detalhadamente, no capítulo subsequente.

³⁷ GREENLEAF, Graham - A world data privacy treaty? ‘Globalisation’ and ‘modernisation’ of Council of Europe Convention 108. **Emerging challenges in privacy law: comparative perspectives**, pp. 92-140. Cambridge: Cambridge University Press, 2014. P. 95.

³⁸ DONEDA, Danilo - A Proteção Dos Dados Pessoais Como Um Direito Fundamental. *In: Espaço Jurídico*, v. 12, n.º 2, jul./dez. 2011, pp. 91-108. P. 102.

as condições de trabalho oferecidas e para a sua própria competitividade mundial. Assim, como evidenciado pela Comissão Europeia, “*Na sociedade de hoje, o acesso à Internet tornou-se um direito fundamental para todos os cidadãos (...)*”³⁹.

A integração económica e social, indissociavelmente conectada com o mercado interno da UE fomentou um maior fluxo transfronteiriço de dados pessoais. A evolução tecnológica e a utilização, cada vez mais acentuada e com diversos fins, da *Internet*, conduziram a que urgisse a necessidade de regular a “questão digital” e as repercussões que esta tem na privacidade das pessoas no mundo *online*.

O Tratado de Lisboa⁴⁰, que entrou em vigor em dezembro de 2009, introduziu uma **base jurídica** para a proteção de dados pessoais na UE, concretamente o artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que consagra que “*Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*”. No mesmo artigo, o n.º 2 estabelece que “*O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados.*”.

No Tratado da União Europeia (TUE), o artigo 39.º também diz respeito a esta matéria, estabelecendo que “*Em conformidade com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º 2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo, e à livre circulação desses dados (...).*”.

³⁹ Comissão Europeia - Para uma Europa do Conhecimento. A União Europeia e a Sociedade da Informação. **Série: A Europa em Movimento**. Luxemburgo, 2003. P. 4.

⁴⁰ Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de dezembro de 2007. Publicado no JO n.º C306, de 17/12/2007, pp. 1-271.

Além da consagração de uma base jurídica explícita para esta matéria, o Tratado de Lisboa conferiu à CDFUE⁴¹, proclamada em 2000, **efeito jurídico vinculativo**. Esta consagra, respetivamente, nos artigos 7.º e 8.º, o respeito pela vida privada e familiar e a proteção de dados pessoais.

O art. 8.º da Carta consagra o direito à proteção de dados, do seguinte modo:

- “1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*
- 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.*
- 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”*

Por isso mesmo, o direito à proteção de dados pessoais, consagrado no artigo 8.º da Carta, é considerado um direito fundamental, juridicamente vinculativo para as instituições da UE e para os Estados-Membros quando apliquem o direito da União. Tendo em conta estas alterações, a Comissão, através de uma Comunicação de 2010⁴², comprometeu-se a dar grande prioridade ao **respeito pelo direito fundamental à proteção de dados na União** em todas as suas políticas, reforçando a vertente do mercado interno e facilitando o livre fluxo de dados pessoais, modernizando, assim, o quadro normativo em matéria de proteção de dados.

⁴¹ Carta dos Direitos Fundamentais da União Europeia, assinada e proclamada no Conselho Europeu de Nice de 7 de dezembro de 2000. Publicada no JO n.º C202, de 07/06/2016, pp. 389–405.

⁴² Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia. COM(2010) 609 final.

O Tratado de Lisboa proporcionou, desta forma, uma revisão das regras europeias de proteção de dados pessoais, e ajudou a harmonizar as normas aplicáveis e a colmatar lacunas existentes no que concerne à proteção de dados.

Evidenciando a importância destas regras, refere o Comité Económico e Social Europeu, no seu Parecer de 2011, sobre a mencionada Comunicação da Comissão, que *“A livre circulação de dados pessoais no mercado interno é necessária para o bom funcionamento deste mercado, mas constitui uma ameaça potencial à privacidade dos dados (...). São necessárias salvaguardas específicas, como a obrigação dos responsáveis pelo tratamento de dados de prestarem contas quanto à troca internacional de dados e a utilização da encriptação para os dados mais sensíveis.”*⁴³

Para a Autoridade Europeia para a Proteção de Dados (AEPD), entidade supervisora independente que assegura que as instituições e órgãos da UE respeitam as suas obrigações no que respeita à proteção de dados, o ponto de partida para esta proteção é a dignidade da pessoa, que transcende questões de mero cumprimento da lei. O ponto de referência é constituído pelos princípios que estão no cerne da proteção de dados, enunciados no art. 8.º da CDFUE.⁴⁴

Porém, antes de chegarmos ao patamar regulatório em que a Carta possui valor vinculativo e a proteção de dados pessoais encontra uma base legal, vários passos foram tomados, gradualmente, neste sentido, nomeadamente através de Resoluções, Recomendações, Comunicações e outros instrumentos relevantes, que devem ser referidos.

3.2.2. Instrumentos Relevantes até à adoção da Diretiva 95/46/CE

Inicialmente, nos países europeus, as regras que regulavam o tratamento

⁴³ Ponto 3.1.1. do Parecer do Comité Económico e Social Europeu sobre a “Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia”, n.º 2011/C 248/21.

⁴⁴ Recomendação da AEPD sobre as opções da União Europeia para a reforma da proteção de dados, n.º 2015/C 301/01.

automatizado de dados eram consagradas de duas formas: como atos *ad hoc* ou como provisões a nível constitucional. Os casos de países que adotaram atos *ad hoc* tiveram lugar a partir dos anos 70 e 80, e são exemplos disso a Alemanha, a Suécia e a França. Modelos que seguiram a via constitucional para consagração de regras de tratamento automatizado de dados pessoais foram, por exemplo, o de Áustria, de Espanha e de Portugal.

Coloca-se, nestes parâmetros, a dúvida sobre qual o meio mais adequado de regulação da proteção de dados. A modalidade que melhor se parece adequar para esta regulação na UE é a legislativa, apesar de vários autores proporem uma modalidade alternativa de regulação, tal como o mercado, em que, de acordo com a teoria económica, os dados pessoais estariam nas mãos de quem mais os valoriza e oferecer-se-ia um melhor mecanismo de atribuição de direitos aos indivíduos. Porém, a legislação continua a ser o meio primordial de regulação utilizado pela UE para responder ao fenómeno do tratamento de dados pessoais.⁴⁵

Não obstante, até se chegar à adoção de legislação específica sobre a proteção de dados pessoais, a UE percorreu um longo caminho, devendo assinalar-se alguns dos passos mais relevantes.

Para mitigar a dominância de mercado dos EUA, a Comissão, publicou, em 1973, uma Comunicação ao Conselho⁴⁶, em que sugere a necessidade de criar uma base para o desenvolvimento da utilização industrial de tratamento de dados, que levaria a indústria europeia a ser mais competitiva a nível global. Esta Comunicação referia, ainda, a carência de medidas comuns de proteção do cidadão e enfatizava a essencialidade de regras de acesso à informação e a importância constitucional destas matérias.

Porém, este assunto apenas foi tratado em 1974, através da intervenção de um Membro do Parlamento Europeu, Pierre Bernard Cousté, que submeteu uma questão oral ao Conselho sobre o assunto da proteção da privacidade dos cidadãos e

⁴⁵ LYNSKEY, Orla – *Op. cit.*, 2015, p. 4.

⁴⁶ Comunicação da Comissão ao Conselho: Uma Política Comunitária de Tratamento de Dados. Documento n.º SEC(73) 4300 final.

anunciou que o Comité de Assuntos Económicos e Monetários estava a preparar um relatório sobre a política de tratamento de dados da Comunidade.⁴⁷

Em 1975 e em 1976, foram adotadas duas Resoluções do Parlamento Europeu⁴⁸ sobre proteção dos direitos dos indivíduos face ao progresso técnico em desenvolvimento no campo do tratamento automático de dados que defendem a urgência da adoção de uma Diretiva e outra legislação europeia relevante sobre a liberdade individual e o tratamento de dados, que evitasse legislação conflituante dos Estados-Membros. Foi também instituído um sub-comité no Parlamento Europeu para tratar questões relacionadas com esta temática, denominado “*Data Processing and Individual Rights Sub-committee*”, que esteve em funções entre 1977 e 1979.

Igualmente, foi estabelecida uma “*Working Party on Data Processing and Protection of Liberties*”, que reconheceu a proteção da privacidade como matéria de interesse da Comunidade Europeia desde os anos 70.

A partir deste momento, foram vários os movimentos concretos para a integração da proteção de dados na política da UE. Em 1979, foi aprovada uma Resolução do Parlamento Europeu⁴⁹, na sequência de um estudo sobre a necessidade de elaborar uma legislação comunitária que uniformizasse as regras relativas a erros ou abusos cometidos informaticamente. Nesta Resolução propunha-se a criação de um direito de informação do interessado, e que sobre os Estados recaísse a obrigação de garantir aos seus cidadãos o exercício dos seus direitos relativos à proteção de dados sem custos e dentro de um prazo razoável.

⁴⁷ FUSTER, Gloria González – *op. cit.*, 2014, pp. 113-114.

⁴⁸ Resolução do Parlamento Europeu sobre a proteção dos direitos do indivíduo face aos desenvolvimentos tecnológicos no campo do tratamento automático de dados, 1975, publicada no JO n.º C60/48; e Resolução do Parlamento Europeu de 8 de abril de 1976 sobre a proteção dos direitos do indivíduo face aos desenvolvimentos tecnológicos no campo do tratamento automático de dados, 1976, publicada no JO n.º C100/27.

⁴⁹ Resolução sobre a proteção dos direitos do indivíduo face a desenvolvimentos tecnológicos no tratamento de dados, adotada a 8 de maio de 1979, publicada no JO n.º C140, de 05/06/1979, pp. 34-38.

Em 1981, a Comissão Europeia adotou uma Recomendação⁵⁰ relativa à Convenção n.º 108, do Conselho da Europa, na qual aconselhou aos Estados-Membros a assinatura da mesma antes do final de 1982, e referiu que, caso essas assinaturas não se concretizassem, seria adotado um documento similar no âmbito da UE, uma vez que era extremamente relevante que houvesse uma uniformização da legislação sobre proteção de dados entre os Estados-Membros. A Comissão afirma, no 2.º considerando da referida Recomendação que “*A protecção dos dados é uma componente necessária da protecção do indivíduo. Tem a natureza de um direito fundamental (...)*”.⁵¹

Novamente, em 1982, o Parlamento Europeu pronunciou-se sobre estas questões, através de uma Resolução de 9 de março⁵².

Ainda assim, apesar da importância fulcral da Convenção n.º 108, esta não podia ser considerada um instrumento suficiente, por si só, para a necessária harmonização das legislações dos Estados-Membros da UE a fim de fomentar a livre circulação da informação no mercado interno europeu, pelo facto de conter regras demasiado gerais e admitir exceções aos princípios que consagra.⁵³

Desta forma, a Comissão Europeia, no final dos anos 80, decidiu introduzir as suas próprias propostas legislativas, devido a divergências entre os Estados-Membros.

Alexandre de Sousa Pinheiro chama a atenção para a relação entre a proteção de direitos fundamentais e a atividade económica da Comunidade Europeia que, por ser uma comunidade económica e comercial, deve mitigar os efeitos secundários das suas atividades, protegendo os cidadãos europeus através de regras gerais,

⁵⁰ Recomendação da Comissão n.º 81/679/CEE, relativa a uma convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, publicada no JO n.º L246/31, de 29/08/1981, p. 77.

⁵¹ Sublinhado nosso.

⁵² Resolução do Parlamento Europeu sobre a proteção do indivíduo face a desenvolvimentos tecnológicos no tratamento de dados, publicada no JO n.º C87, de 09/03/1982, pp. 39-41.

⁵³ GONÇALVES, Maria Eduarda – Direito da Informação: Novos direitos e formas de regulação na Sociedade da Informação. Coimbra: Almedina, 2003, p. 98.

equivalentes e eficazes no âmbito da proteção de dados. Porém, a prossecução dos objetivos do mercado interno não podia ser afetada por obstáculos jurídicos nacionais relacionados com a proteção de dados. Estas indicações, efetuadas também pelo Parlamento, sugerem um necessário “mínimo conteúdo material” do direito à proteção de dados.⁵⁴

Porém, além de muitos Estados-Membros não assinarem nem ratificarem a Convenção n.º 108, não dispunham sequer de qualquer regime jurídico dedicado à temática da proteção de dados no que toca ao tratamento de dados pessoais. Aliás, apenas seis Estados-Membros haviam assinado a Convenção até ao final de 1982 e nenhum Estado-Membro a tinha ratificado no final do mesmo ano.⁵⁵

3.2.3. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro

Apesar de toda a atenção dispensada à temática da proteção dos dados pessoais, apenas nos anos 90 foi promovido um pacote de propostas da Comissão relacionadas com esta matéria. O principal instrumento sobre proteção de dados pessoais na UE foi a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados⁵⁶. Esta Diretiva resultou de uma combinação dos diversos instrumentos internacionais existentes nesta matéria e constituiu um importante marco para o mercado interno e para a proteção de direitos fundamentais na UE, visto que formulou um nível mínimo de proteção para os dados pessoais e eliminou obstáculos ao fluxo transfronteiriço de dados entre os Estados-Membros.

⁵⁴ PINHEIRO, Alexandre Sousa, *op. cit.*, 2015, p. 578.

⁵⁵ *Working Document of European Parliament*, Documento n.º 1-42/83, Março 1983, p. 2.

⁵⁶ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, publicada no JO n.º L281/31, de 23/11/95. Transposta através da Lei n.º 67/98 de 26/10/1998, publicado no Diário da República, 1.ª Série A, n.º 247, de 1998-10-26. Última alteração pela Lei n.º 103/2015, de 24/08/2015.

Apesar de não acolher a noção de “proteção de dados pessoais”, relegando-a para breves referências no texto, a Diretiva reconhece como objetivo principal, como se observa no considerando 10.º, o de “*assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada*”. Outro dos seus objetivos é proibir restrições ao fluxo livre de dados pessoais entre os Estados-Membros.

Em suma, a Diretiva serve um objetivo económico de facilitação do livre comércio na UE, mas também se baseia na preocupação de assegurar a proteção de direitos fundamentais. Assim, de acordo com Orla Lynskey, a Diretiva opera na premissa de que se um alto nível de proteção de dados pessoais for assegurado em todos os Estados-Membros, então nenhum pode objetar ao livre fluxo desses dados dentro da UE com fundamento em direitos humanos.⁵⁷

Apesar do duplo objetivo, o TJ demonstrava um certo constrangimento na aplicação do objetivo de proteção de direitos fundamentais da Diretiva, o que poderá ser explicado tendo em conta duas considerações⁵⁸. A primeira consideração diz respeito à base legal da Diretiva, a qual, de acordo com o princípio da atribuição, só poderia ser adotada se a UE demonstrasse competência expressa conferida pelos Tratados, podendo o legislador adotar medidas deste teor que visem o “estabelecimento e o funcionamento do mercado interno”⁵⁹. Desta forma, e visto que a falta de legislações sobre proteção de dados colocava um obstáculo ao livre movimento desses dados, a Diretiva poderia apoiar-se nesta base legal. Contudo, nada obsta a que se alicerce em mais do que uma base legal se o objetivo da proteção de dados pessoais for indissociável do objetivo económico, o que parece ser o caso.

A segunda consideração prende-se com o facto de a CDFUE, à data, ainda não ter adquirido força vinculativa. Porém, com a entrada em vigor do Tratado de Lisboa, o Tribunal pôde colocar ambos os objetivos em pé de igualdade. Podemos, portanto,

⁵⁷ LYNKEY, Orla – *Op. cit.*, 2015, p. 8.

⁵⁸ *Ibidem*, pp. 58-62.

⁵⁹ Cfr. o art. 114.º do TFUE.

considerar o regime de proteção de dados como uma regulação híbrida, por este motivo.

A Convenção n.º 108 do Conselho da Europa é uma das fontes para a elaboração desta Diretiva. O considerando 11.º desta última refere que se explicita e amplia os princípios da proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada contidos na Convenção n.º 108. Contudo, vai além da Convenção, a qual apenas cobria o tratamento de dados automatizados. Desta Convenção, a Diretiva retirou a fórmula de que a proteção de dados serve a privacidade e que é necessário equilibrar a proteção dos indivíduos com outras exigências.

Como refere Alexandre Sousa Pinheiro, o texto da Diretiva assentou numa rede tão complexa de equilíbrios que levou a que se a classificasse como um “compromisso com arte”. Mais ainda, a Diretiva baseia-se em definições inovadoras, determina novos princípios sobre qualidade de dados e integra outros princípios. O mesmo Autor considera que este texto é mais completo na proteção das liberdades e direitos fundamentais do que a Convenção n.º 108.⁶⁰

Contudo, e apesar dos avanços, os primeiros passos do envolvimento da UE no campo da regulação do tratamento de dados foram marcados por terminologias imprecisas e por perceções incertas quanto ao papel a ser desempenhado pelas Instituições Europeias.⁶¹

Na Diretiva 95/46/CE transparece a ideia de direitos fundamentais ligados à proteção de dados, mas o instrumento europeu que levou esta sistemática mais adiante foi a CDFUE, de 2000, que, além de estabelecer o direito ao respeito pela vida privada e familiar no art. 7.º, consagra, como referido, o direito fundamental à proteção de dados pessoais no art. 8.º.

Este último direito é exercido nos termos previstos pela Diretiva e pode ser objeto de restrições nas condições estabelecidas no art. 52.º da Carta. Além disso, o art. 8.º

⁶⁰ PINHEIRO, Alexandre Sousa, 2015, *op. cit.*, pp. 614-617.

⁶¹ FUSTER, Gloria González – *op. cit.*, 2014, p. 155.

da Carta baseia-se no art. 286.º do Tratado que institui a Comunidade Europeia (atual art. 16.º do TUE) e na Diretiva 95/46/CE, bem como no art. 8.º da CEDH e na Convenção n.º 108 do Conselho da Europa.⁶²

Para assegurar uma proteção de dados mais eficaz, seria necessária uma melhor aplicação da própria Diretiva, através de uma combinação de instrumentos políticos, uma melhor comunicação com a sociedade a uma aplicação mais estrita da legislação em matéria de proteção de dados. Além disto, seria ainda precisa uma mais eficiente interação com a própria tecnologia. De igual modo, a necessidade de proteger eficazmente os dados pessoais pode impor restrições à utilização destas novas tecnologias, pelo que esta interação tem duas faces: a tecnologia influencia a legislação e a legislação influencia a tecnologia.⁶³

Assinala-se, ainda, a importância do “*Article 29 Data Protection Working Party*”, órgão de natureza consultiva, criado através do art. 29.º da Diretiva, que se tornou um elemento essencial na definição de políticas e noções sobre proteção de dados.⁶⁴

Apesar de todo este progresso até à adoção da Diretiva, certo é que, à data da adoção deste primeiro instrumento legislativo no campo da proteção de dados na UE, apenas 1% da população da UE utilizava a *Internet* e o motor de busca *Google* ainda não havia sido lançado como serviço. Assim, com o passar dos anos, urgia a necessidade de atualização das regras europeias, de modo a fazer face aos desenvolvimentos tecnológicos e à utilização maciça de *Internet* a nível mundial.⁶⁵

⁶² Conselho da União Europeia – Carta dos Direitos Fundamentais da União Europeia: Anotações relativas ao texto integral da Carta. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 2001, p. 26

⁶³ Parecer da AEPD respeitante à Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados. Publicado no JO n.º C255/01, de 27/10/2007.

⁶⁴ Com a adoção do novo Regulamento Geral, este Grupo será substituído pelo Comité Europeu para a Proteção de Dados, regulado no art. 68.º do referido diploma.

⁶⁵ LYNSKEY, Orla – *Op. cit.*, 2015, p. 4.

Existe, assim, uma necessidade de atualizar as regras de proteção de dados constantes da Diretiva, até porque, antes da entrada em vigor do Tratado de Lisboa, a legislação relativa à proteção de dados no Espaço de Liberdade, Segurança e Justiça (ELSJ) estava dividida entre o primeiro pilar (proteção de dados para fins privados e comerciais, com a utilização do método comunitário) e o terceiro pilar (proteção de dados para o domínio da aplicação da lei, ao nível intergovernamental). Consequentemente, o processo de decisão esteve sujeito a normas diferentes.

Desta forma, estão em vigor diversos instrumentos legislativos que regulam a matéria da proteção de dados pessoais e que incluem instrumentos do antigo primeiro pilar, como a Diretiva 95/46/CE relativa à proteção de dados, a Diretiva 2002/58/CE relativa à privacidade e o Regulamento n.º 45/2001/CE relativo ao tratamento de dados pessoais por instituições e órgãos comunitários, assim como instrumentos do antigo terceiro pilar como a Decisão-Quadro 2008/977/JAI do Conselho, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal⁶⁶. A estrutura de pilares desapareceu com o Tratado de Lisboa, o qual fornece uma base mais sólida para o desenvolvimento de um sistema de proteção eficaz de dados. E, atualmente, tem sido encetada uma reforma geral sobre a regulação desta temática.⁶⁷

3.2.4. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados)

Como já foi referido, os progressos tecnológicos e a globalização alteraram profundamente o modo de recolha, acesso e utilização dos dados pessoais, tal como se admite na Comunicação da Comissão Europeia ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre

⁶⁶ Publicada no JO n.º L350/60, de 30/12/2008. Esta Decisão-Quadro foi, entretanto, revogada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

⁶⁷ MILT, Kristiina - Proteção dos Dados Pessoais. Parlamento Europeu - Fichas técnicas sobre a União Europeia, 2017.

“Uma abordagem compreensiva sobre a proteção de dados pessoais na União Europeia”⁶⁸, de 2010, na qual se afirma que “O objetivo das regras dos presentes instrumentos de proteção de dados na UE é **proteger os direitos fundamentais** das pessoas singulares e, em particular, o seu **direito à proteção de dados pessoais**, em linha com a Carta dos Direitos Fundamentais da UE.”⁶⁹

Além disso, os Estados-Membros transpuseram a Diretiva 95/46/CE de forma diferente, o que levou a divergências na sua aplicação.

Tendo em conta todos os motivos *supra* referenciados, a 25 de janeiro de 2012, a Comissão adotou um pacote de reforma legislativa das regras da UE em matéria de proteção de dados, que conta com a Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave⁷⁰; e com um Regulamento Geral de Proteção de Dados, o Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016⁷¹ que contém as regras gerais em matéria de proteção de dados.

Este Regulamento pretende reforçar o controlo dos titulares de dados sobre os seus dados pessoais, respeitando os direitos fundamentais das pessoas e aproveitando para reforçar a confiança dos consumidores e a economia digital da Europa. O objetivo final passa por impulsionar o almejado crescimento, emprego e inovação na UE.

O novo Regulamento, que, de acordo com o seu art. 99.º, entra em vigor a 5 de maio de 2018, determina um novo âmbito de aplicação territorial, abrangendo

⁶⁸ Cfr. COM(2010) 609 final, de 4 de novembro de 2010.

⁶⁹ Cfr. a referida Comunicação, p. 5. (Sublinhado nosso).

⁷⁰ Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicada no JO n.º L119/89, de 04/05/2016.

⁷¹ Regulamento (UE) n.º 2016/ 679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicado no JO n.º L119/1, de 04/05/2016.

também as empresas não estabelecidas na UE que ofereçam bens ou serviços ou monitorizem o comportamento dos cidadãos europeus. Além disso, atualiza as definições legais, reforça o papel do consentimento como forma de legitimar o tratamento de dados, consagra novos princípios gerais e reforça efetivamente os direitos das pessoas e o papel dos responsáveis pelo tratamento.

Desta forma, através do reforço de certos direitos fundamentais levado a cabo pelos novos instrumentos regulatórios, pode ser concluído que “*independentemente dos seus méritos e insuficiências, não deixa de ser verdade que a divulgação do projeto de Regulamento marca a segunda geração de instrumentos regulatórios da proteção de dados a nível da UE - um facto longe de ser evidente há quinze anos e constitui uma verdadeira causa de celebração dos **direitos humanos***”.⁷²

A substituição da Diretiva por um Regulamento pode conduzir a uma europeização das regras de proteção de dados entre os Estados-Membros.⁷³ Isto porque, sendo o Regulamento um instrumento de carácter geral, obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros, de acordo com o art. 288.º do TFUE, será evitada a discricionariedade conferida aos Estados-Membros aquando da transposição das Diretivas para as respetivas ordens jurídicas internas.

Esta europeização do Direito da Informação comporta, também, uma consequência adicional: o confronto entre diversas culturas jurídicas, como é o caso dos países de *civil law*, que preferem uma iniciativa pró-ativa do Legislador na regulação de novos problemas que sejam levantados neste campo, e dos países de *common law*, os quais denotam preferência por desenvolvimentos incrementais progressivos, tendo por base os Tribunais.⁷⁴

⁷² HERT, Paul e PAPAKONSTANTINO, Vagelis - The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. In: **Computer Law & Security Review**, n.º 28, Issue 2, 2012, pp. 130-142. P. 142. (Sublinhado nosso).

⁷³ LYNSKEY, Orla – *op. cit.*, 2015, p. 7.

⁷⁴ GONÇALVES, Maria Eduarda – *Op. cit.*, 2003, p. 200.

Importa referir a estrutura do Regulamento Geral:

- ✚ CAPÍTULO I: Disposições gerais
- ✚ CAPÍTULO II: Princípios
- ✚ CAPÍTULO III: Direitos do titular dos dados
- ✚ CAPÍTULO IV: Responsável pelo tratamento e subcontratante
- ✚ CAPÍTULO V: Transferências de dados pessoais para países terceiros ou organizações internacionais
- ✚ CAPÍTULO VI: Autoridades de controlo independentes
- ✚ CAPÍTULO VII: Cooperação e coerência
- ✚ CAPÍTULO VIII: Vias de recurso, responsabilidade e sanções
- ✚ CAPÍTULO IX: Disposições relativas a situações específicas de tratamento
- ✚ CAPÍTULO X: Atos delegados e atos de execução
- ✚ CAPÍTULO XI: Disposições finais

De toda a sistematização do Regulamento, compete-nos analisar, mais aprofundadamente, e mais adiante, o Cap. III relativo aos “Direitos do titular dos dados”.

3.2.5. Direito à proteção de dados pessoais como Direito Fundamental no âmbito da UE

Em suma e reforçando a importância da proclamação da CDFUE, com um artigo relativo ao direito à proteção de dados pessoais, como vinculativa e com força de Tratado, e, ainda, o estabelecimento de uma única base jurídica para a regulação desta temática, no art. 16.º do TFUE, devemos considerar este direito como um verdadeiro direito fundamental.

Apesar da falta de uma tradição constitucional comum da proteção de dados como direito fundamental entre os Estados-Membros da UE, a inclusão deste direito na Carta reflete o seu reconhecimento como direito fundamental independente. Não

obstante o Memorando Explicativo da Carta⁷⁵ não explicitar os motivos desta inclusão, certo é que consagrou este direito de forma autónoma, baseando-se nos Tratados, na Diretiva 95/46/CE, na art. 8.º da CEDH e na Convenção n.º 108 do Conselho da Europa.

Aliás, se dúvidas houvesse, o TJ pronunciou-se, em 2003, sobre esta questão no Acórdão *Rundfunk*. Neste, o Tribunal decidiu, nomeadamente, que “(...) *as disposições da Directiva 95/46, na medida em que regulam o tratamento de dados pessoais susceptíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais que, segundo jurisprudência constante, são parte integrante dos princípios gerais de direito cujo respeito é assegurado pelo Tribunal de Justiça* (...)”⁷⁶.

Mais especificamente, no Acórdão *Promusicae*, de 2008, o Tribunal incorporou a análise da proteção de dados na sua decisão e referiu-se-lhe como **“direito fundamental”** pela primeira vez. Neste sentido, refere a possibilidade de o órgão jurisdicional de reenvio poder convocar o direito fundamental que “garante a proteção dos dados pessoais e, portanto, da vida privada”. Conclui que compete aos Estados-Membros, na transposição de diretivas, zelar por que seja seguida uma interpretação que permita assegurar o justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária.⁷⁷

⁷⁵ Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF> (Consultado a 05/06/2017).

⁷⁶ Ponto 68 do Acórdão *Rundfunk*, de 20 de maio de 2003, relativo aos Processos Apensos C-465/00, C-138/01 e C-139/01.

⁷⁷ Pontos 63 e 68 do Acórdão *Promusicae*, de 29 de janeiro de 2008, relativo ao Processo C-275/06.

Tendo em conta todas as regras europeias relativas à proteção de dados pessoais, especificamente até no âmbito da *Internet*, podemos, inclusivamente, afirmar que “Direito europeu de *Internet* existe, de facto”⁷⁸.

E não parecem restar dúvidas sobre a interpretação do direito à proteção de dados pessoais como um direito fundamental na UE.

3.3. Fontes de Direito Nacional

A nível nacional, são diversas as fontes jurídicas do direito à proteção de dados pessoais, concretamente, de Direito Constitucional (a CRP), de Direito Penal (nomeadamente, o art. 193.º do Código Penal referente à “Devassa por meio de informática”), de legislação específica sobre a matéria (como é o caso da Lei n.º 67/98) e de Direito Civil (concretamente, com o art. 80.º do Código Civil que estabelece o direito à reserva sobre a intimidade da vida privada como um direito de personalidade).⁷⁹ Merecem aprofundamento as fontes constitucionais e as provenientes de legislação específica.

3.3.1. Constituição da República Portuguesa

O caso particular português releva particularmente, pelo facto de ter sido o primeiro país europeu a consagrar disposições específicas sobre o tratamento automatizado de dados na Constituição: o art. 35.º da CRP de 1976, que serviu de fonte de inspiração para o reconhecimento constitucional do direito de acesso aos dados pessoais por diversos outros países.⁸⁰

⁷⁸ POULLET, Yves – Views from Brussels: A European *Internet* Law. In: CHATILLON, Georges (Ed.) - ***Internet International Law: International and European Studies and Comments***. Bruxelas: Bruylant, 2005, pp. 123-165. P. 165.

⁷⁹ VASCONCELOS, Pedro Pais – Protecção de Dados Pessoais e Direito à Privacidade. In **Direito da Sociedade da Informação e Direito de Autor**, V. I, 1999, pp. 241-253, pp. 241-243.

⁸⁰ FUSTER, Gloria González – *op. cit.*, 2014. Pp. 55-67.

A CRP tem sido, internacionalmente, elogiada pelo facto de consagrar os Direitos e Liberdades Fundamentais com elevado grau de detalhe.⁸¹ Além do mais, a CRP tipificou, de forma precisa, vários direitos fundamentais quanto ao tratamento informatizado de dados pessoais, não se limitando a enunciar um escasso número de posições jurídicas subjetivas ou a impor deveres. Para culminar, o estatuto constitucional destes direitos fundamentais sai reforçado ao lhes ser aplicável o regime particularmente sólido dos Direitos, liberdades e garantias, em geral.⁸²

Quando Portugal adotou a CRP em 1976, esta contou com um artigo, o 35.º, relativo à “utilização da informática”, que teve como objetivo proteger os dados pessoais quando as bases de dados se começaram a banalizar e evitar a devassa da reserva da vida privada, porém, ainda de forma ténue. À data, Portugal era membro da ONU, mas ainda não do Conselho da Europa.

De acordo com estudos da Comissão Europeia, em Portugal, no início dos anos 2000, apenas 2/3 das empresas tinham ligação à *Internet* e só 1/3 tinha o seu próprio sítio *web*. Outrossim, somente 5% das empresas portuguesas utilizavam a *Internet* para os seus fornecimentos ou serviços.⁸³

Porventura por este motivo, Portugal apostou, inicialmente, numa política de forte prevenção face à informática, tendo em vista os riscos da criação de serviços de registos informáticos, e não uma preocupação pela proteção eficiente de dados pessoais. Esta foi a génese da primeira versão do art. 35.º da CRP. Devido à pouca atenção concedida a este problema, a CRP apenas contou, aquando da sua elaboração, com um projeto partidário que previa uma norma relativa à proteção de dados pessoais.⁸⁴

⁸¹ FUSTER, Gloria González – *Op. cit.*, 2014, p. 66.

⁸² GOUVEIA, Jorge Bacelar – *Op. cit.*, 1991, p. 706.

⁸³ Comissão Europeia - Para uma Europa do Conhecimento. A União Europeia e a Sociedade da Informação, *Op. cit.*, 2003, p. 16.

⁸⁴ LOPES, Joaquim de Seabra – O artigo 35.º da Constituição: Da Génese à Atualidade e ao Futuro Previsível. In: **Fórum de Proteção de Dados**, n.º 2, 2016, pp. 14-49. Pp. 17-18.

O n.º 2 (posterior n.º 3) do mencionado artigo proibia absolutamente o tratamento de dados da vida privada, o que parece exagerado, uma vez que este conceito abrange informações banais sobre a pessoa que importam para certos serviços, como é o caso do estado civil. Além disto, com a revisão constitucional de 1982, o artigo proibiu, ainda, o acesso de terceiros a ficheiros com dados pessoais, a sua interconexão e os fluxos transfronteiriços de dados. Esta situação alterou-se aquando da adoção da Convenção n.º 108, a qual foi assinada por Portugal em 1981. No n.º 2 do art. 12.º desta Convenção é definido que “*Uma Parte não poderá, com a exclusiva finalidade de protecção da vida privada, proibir ou submeter a autorização especial os fluxos transfronteiras de dados de carácter pessoal com destino ao território de uma outra Parte.*”. Da mesma forma, as Diretrizes da OCDE, das quais era parte Portugal desde 1980, recomendavam o livre fluxo dos dados. Assim, não podia a CRP proibir o fluxo transfronteiriço de dados pessoais.

Por este motivo, com a revisão constitucional de 1989, o artigo passou a proibir o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e a sua interconexão, sem qualquer referência a proibições a fluxos transfronteiriços, remetendo este assunto para o novo n.º 6, o qual consagrou que “*A lei define o regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*”.

Então, foi também adotada a Lei n.º 10/91 de 29 de abril, a Lei da Protecção de Dados Pessoais face à Informática⁸⁵.

Graças a estas modificações, Portugal pôde ratificar, em 1993, a Convenção n.º 108, apesar de, como refere Joaquim de Seabra Lopes, duas algumas das disposições da Lei n.º 10/91 conflituarem com as normas da Convenção.⁸⁶

Entretanto, a nível da UE, foi publicada a referida Diretiva 95/46/CE, a qual dispõe de um artigo, o art. 32.º, que confere aos Estados-Membros o prazo de três anos

⁸⁵ Publicada no Diário da República, 1.ª Série A, n.º 98, 1991-04-29, pp. 2366-2372.

⁸⁶ LOPES, Joaquim de Seabra – *op. cit.*, 2016. P. 34.

para adotarem disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à Diretiva. Porém, mais uma vez, Portugal não conseguiu cumprir este prazo, pois o art. 8.º da Diretiva previa um conjunto de situações em que o tratamento de certos dados deveria ser permitido, enquanto a CRP proibía o tratamento de dados em diversos casos. Procedeu-se, então, a uma nova revisão constitucional, a de 1997, na qual se alterou e ampliou o art. 35.º, e o seu n.º 3 passou a ter a seguinte redação: “*A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresse do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*”.

Quanto ao novo Regulamento, Joaquim de Seabra Lopes defende que é necessária uma nova alteração do art. 35.º da CRP, de modo a não conflitar com o normativo europeu. Estes conflitos dirão respeito, nomeadamente, à referência à “lei”, a qual deverá ser modificada, de modo a abranger as normas comunitárias e ao n.º 3 do art. 35.º da CRP que irá chocar, novamente, com as regras europeias, uma vez que o Regulamento prevê mais condições de não aplicabilidade da proibição de tratamento de certos dados.⁸⁷

Assim, não parece que tenha sido vencida a “informaticofobia” inicial, refletida na epígrafe e nas repetidas proibições. Deve enfatizar-se a vertente positiva da proteção dos dados pessoais dos cidadãos. Seria mais eficaz uma fórmula mais simples e intemporal, que garantisse aos cidadãos a proteção dos seus dados pessoais e tornasse incumbência do Estado a defesa desse direito.⁸⁸

Contudo, e apesar das contingências surgidas no contexto deste artigo com o aparecimento e evolução das redes informáticas e novas tecnologias, é inquestionável que se densificou um conjunto de direitos fundamentais quanto ao tratamento de dados pessoais, cujo objetivo passa por impedir o entendimento da pessoa como um objeto de informações.

⁸⁷ *Ibidem*, pp. 42-44.

⁸⁸ Para mais informações, cfr. LOPES, Joaquim de Seabra – *op. cit.*, 2016. P. 46.

Para aferir do carácter destas regras e direitos como matéria fundamental, deve referir-se a localização sistemática, tanto do art. 26.º que consagra a reserva da intimidade da vida privada e familiar, como do art. 35.º sobre a utilização da informática e que inclui o direito de acesso aos dados informatizados. Ambos estes direitos estão incluídos no “Cap. I – Direitos, liberdades e garantias pessoais”, do “Título II – Direitos, liberdades e garantias”, da “Parte I – Direitos e Deveres fundamentais”, o que revela a fundamentalidade destas normas.

Na esteira de Gomes Canotilho e Vital Moreira, este conjunto de direitos fundamentais englobados no art. 35.º arranca de alguns “direitos-mãe” em sede de direitos, liberdades e garantias, tais como o direito à dignidade da pessoa humana, o desenvolvimento da personalidade, a integridade pessoal e a autodeterminação informativa. Neste sentido, estes direitos conectam-se com o tratamento informático de dados pessoais e originam variadas restrições a estas operações. Reconhece-se e garante-se, portanto, um conjunto de direitos fundamentais em matéria de defesa contra o tratamento informático de dados pessoais e esta proteção analisa-se, fundamentalmente, através de três direitos, a saber, o direito de acesso, o direito de sigilo e de não interconexão e o direito ao não tratamento informático de certos tipos de dados pessoais.⁸⁹

Concluem, deste modo, que este feixe de direitos fundamentais densifica o moderno direito à autodeterminação informacional, conferindo a cada pessoa o direito de controlar a informação disponível a seu respeito.

Em suma, a nível constitucional, importa referenciar o art. 26.º relativo ao direito à reserva da intimidade da vida privada e familiar, o mencionado art. 35.º sobre a utilização da informática e o n.º 2 do art. 268.º que respeita ao direito de acesso aos registos e arquivos administrativos.

3.3.2. Lei n.º 10/91, de 29 de abril e Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais face à Informática)

⁸⁹ CANOTILHO, José Gomes e MOREIRA, Vital – Constituição da República Portuguesa Anotada, Vol. I, 4.ª ed. revista. Coimbra: Coimbra Editora, 2007. P. 551.

A nível legislativo, a já mencionada Lei n.º 10/91 de 29 de abril foi a primeira Lei de Proteção de Dados (LPD), adotada na sequência do Acórdão do TC n.º 182/89, de 2 de março de 1989⁹⁰, que deu por verificado o não cumprimento da Constituição por omissão da medida legislativa prevista no n.º 4 do seu art. 35º, necessária para tornar exequível a garantia constante do n.º 2 do mesmo artigo, ou seja, por inexistência de uma lei que regulasse os aspetos da proteção de dados pessoais.

Mais tarde, foi adotada a Lei n.º 67/98, de 26 de outubro, que transpôs a Diretiva 95/46/CE, mas não foi muito além do instrumento europeu. De acordo com o n.º 1 do art. 4.º da referida Lei, esta aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados.

Estabelece-se um princípio geral de proibição de tratamento de dados pessoais, mas admite-se que o mesmo seja efetuado quando se verifique alguma das suas condições de legitimidade, elencadas no art. 6.º. Quando alguma das condições se encontra preenchida, terão que se cumprir os princípios gerais de proteção para os tratamentos de dados. Assim, seguimos o entendimento da doutrina que considera que a licitude do tratamento de dados pessoais depende do teste duplo quanto à fundamentação do tratamento (o que se afere perante o art. 6.º) e quanto à qualidade dos dados (que se verifica de acordo com o art. 5.º).

Alguns Autores criticam esta Lei na medida em que parece não atender ao facto de os meios informáticos potenciarem a intromissão na vida privada, uma vez que a disciplina que impõe é generalizante e nada especifica quanto ao meio em causa, e não parece refletir o objetivo da proteção da personalidade que se encontra, constantemente, sob ameaça de devassa.⁹¹

⁹⁰ Decorrente do Processo n.º 298/87.

⁹¹ ASCENSÃO, José de Oliveira – *Op. cit.*, 2001, pp. 271-272.

3.3.3. Direito à proteção de dados pessoais como Direito Fundamental no âmbito nacional

A liberdade e a justiça, em ambiente de segurança, tal como previstas no art. 28º da DUDH e no art. 273.º da CRP, apenas são prosseguidas se Portugal defender os valores da democracia e do respeito pelos direitos humanos. Ora, a defesa nacional abrange a segurança das pessoas relacionada com a defesa dos seus direitos, liberdades e garantias, definindo-se, assim, a República Portuguesa como um Estado de Direito Democrático. Por sua vez, a defesa dos direitos fundamentais envolve também a proteção da privacidade, preocupação constitucional prevista no direito à reserva da intimidade da vida privada e à sua imagem.⁹²

A CRP consagrou um direito à autodeterminação informativa ou à proteção de dados que tutela o interesse do controlo sobre os dados pessoais. Este direito nasce para garantir o direito à intimidade da vida privada no que ao tratamento de dados pessoais diz respeito. Contudo, este direito tem evoluído e já não se trata apenas de um direito de proteção de sentido negativo, na aceção de que resguarda o cidadão de intromissões não autorizadas de terceiros nas suas informações, apresentando-se, atualmente, como um verdadeiro Direito Fundamental e um direito especial de personalidade. Constitui, assim, mais do que um direito de defesa, um direito “ofensivo”, de controlar os dados pessoais e de definir quando, como e a quem podem ser transmitidos.⁹³

Assim, a proteção de dados pessoais deve ser encarada como uma verdadeira liberdade, na lógica de que consiste num poder de dispor das informações, protegendo-se o cidadão dos perigos que o uso da informática lhes pode causar.

O art. 35.º da CRP consagra, destarte, um conjunto de direitos que impede que as pessoas passem a ser encaradas como um “*simples objecto de informações*”.⁹⁴

⁹² VAZ, Ana - Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais. In: **Nação e Defesa**, n.º 117, 3.ª Série, 2007, pp. 35-63. P. 37.

⁹³ CASTRO – *Op. cit.*, 2005. Pp. 27-28.

⁹⁴ *Ibidem*, p. 32.

Assim, também na Ordem Jurídica Portuguesa, este direito constitui um verdadeiro Direito Fundamental e engloba o direito a controlar os dados pessoais, posto que as informações individuais de uma pessoa devem ser protegidas, independentemente da sua característica de “íntima” ou não.⁹⁵

⁹⁵ MONIZ, Helena – Notas sobre a Protecção de Dados Pessoais perante a Informática (O caso especial dos dados pessoais relativos à saúde). *In: Revista Portuguesa de Ciência Criminal*, Ano 7, Fasc. 2.º, Abril-Junho 1997, pp. 231-298. Pp. 251-252.

4. ENQUADRAMENTO AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS NO REGULAMENTO GERAL

Após a análise das fontes jurídicas em que se baseia o atual direito à proteção de dados, definem-se os conceitos subjacentes a esta temática, de acordo com as referidas fontes, das quais merecem especial enfoque as referentes à UE, sobretudo o novo Regulamento Geral.

Na primeira secção do presente capítulo, serão comparados os conceitos de direito à privacidade e o direito à proteção de dados pessoais, para efeitos de concretização destas noções e análise das principais teorias que concernem à autonomização deste último direito ou da sua inclusão no direito à privacidade.

Quanto à segunda secção deste capítulo, referem-se o conceito de “dados pessoais”, as diferentes categorias que se incluem neste termo e a definição de tratamento de dados pessoais, enquanto atividade à qual se aplicam as regras de proteção de dados.

4.1. Conceito do direito à privacidade e evolução até à autonomização do direito à proteção de dados

4.1.1. Conceito e evolução do direito à privacidade

Em primeiro lugar, refere-se, de modo breve, a evolução internacional do termo “privacidade”. O “*right to privacy*” foi autonomizado no artigo “*The right to privacy*”, de Samuel Warren e Louis Brandeis, em 1890, que reclamavam proteção jurídica para certos aspetos da personalidade humana e consideravam que a violação deste direito deveria dar lugar a uma indemnização. Neste sentido, formulava-se este direito de forma negativa, isto é, enquanto liberdade de ser deixado sozinho.⁹⁶

Mais tarde, muitas das questões relacionadas com a privacidade passaram a ser centradas na necessidade de proteção de um direito à autodeterminação

⁹⁶ WARREN, Samuel e BRANDEIS, Louis - The Right to Privacy. In: **Harvard Law Review**, vol. IV, n.º 5, Dez. 1890, p. 5.

informativa.⁹⁷

É importante mencionar que, em diversos instrumentos internacionais, a “*privacy*” e a “vida privada” são tidas como equivalentes.⁹⁸

Tradicionalmente, podem distinguir-se dois aspetos primários da privacidade: a componente da informação, que consiste no abuso da informação privada, e a componente física, que engloba as intrusões não solicitadas ou indesejadas na vida privada. Porém, apenas se prevê uma proteção generalizante.⁹⁹

De acordo com outra conceção, os aspetos mais básicos do direito à privacidade dizem respeito ao direito à identidade, o qual engloba várias qualidades especiais da existência humana e o direito à integridade, cujos elementos protegidos são mais abstratos, como os sentimentos e os pensamentos.¹⁰⁰

Precedida pelos conceitos de inviolabilidade da casa e de confidencialidade da correspondência, a privacidade é difícil de executar porque não é um direito absoluto. A sua proteção deve sempre ser conciliada com valores ou interesses conflitantes, como o direito à privacidade de outrem e interesses públicos.

A “migração das vidas sociais das pessoas para o ambiente virtual” afetou a perspetiva do que é público ou privado e tornou mais importante que as sociedades protejam as preferências dos indivíduos sobre que informações devem tornar-se

⁹⁷ DONEDA, Danilo - *Op. cit.*, 2011, pp. 91–108.

⁹⁸ Sobre a evolução do conceito de “*privacy*” e comparação entre diversos ordenamentos jurídicos, cfr. FUSTER, Gloria González - *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *op. cit.*, 2014.

⁹⁹ MOREHAM, Nicole – Protection against intrusion in English legislation. **Emerging challenges in privacy law: comparative perspectives**, pp. 141-156. Cambridge: Cambridge University Press, 2014. P. 141.

¹⁰⁰ FINK, Udo – Protection of privacy in the EU, individual rights and legal instruments. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 75-91. P. 78.

acessíveis aos outros.¹⁰¹

É inerente à noção de privacidade que, em princípio, cada pessoa mantenha controlo sobre se as suas informações pessoais se tornam disponíveis aos outros.

Uma parte da doutrina defende que a privacidade é ampla demais para constituir um direito e é mais apropriadamente descrita como um valor.¹⁰²

Apesar das consideráveis diferenças culturais e sociais entre as ordens jurídicas, uma característica importante da paisagem legal internacional é o crescente reconhecimento da privacidade, em diversos instrumentos internacionais, como direito humano.

Apesar disto, existem diferentes concepções de privacidade e de noções legais relacionadas que podem gerar ambiguidades, sendo um dos problemas que se enfrenta quanto a este direito a falta de precisão na sua definição.

Além disso, os problemas que se colocam relativamente à legislação que protege a privacidade dizem respeito ao facto de estas tenderem a ser fragmentadas, apresentando-se como relativas a tipos específicos de invasões à privacidade.¹⁰³

O termo privacidade pode ser dividido em categorias básicas, correspondentes aos diferentes sentidos do adjetivo “privado”, do qual a primeira noção deriva.¹⁰⁴

Assim, de acordo com uma primeira aceção, deve proteger-se o que é visto como privado por oposição ao público e, conforme um segundo sentido, a privacidade diz respeito ao que é privado no sentido individual, pessoal ou por conta própria.

A definição de privacidade tem sido, não raras vezes, conectada com a liberdade, a

¹⁰¹ WITZLEB, Normann, LINDSAY, David, PATERSON, Moira e RODRICK, Sharon – *Op. cit.*, 2014. P. 3.

¹⁰² TILBURY, Michael – Privacy: Common Law or Human Right. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 157-179. P. 178.

¹⁰³ WITZLEB, Normann *Et Al* – *Op. cit.*, 2014, p. 14.

¹⁰⁴ FUSTER, Gloria – *Op. cit.*, 2014, p. 22.

individualidade e a autonomia, relativamente aos limites que separam o que pertence ao Estado e o que pertence à vida privada. Foi, ainda, aliada à noção de dignidade humana, no sentido do livre desenvolvimento, que constitui o pressuposto da autodeterminação.¹⁰⁵

Uma outra importante aceção da palavra “privacidade” que não se baseia no adjetivo privado, e que deve incluir-se na lista de classificações, é a privacidade como controlo sobre informação pessoal.¹⁰⁶

Esta última classificação deve considerar o seu contexto histórico que teve início nos EUA. Primeiramente, surgiu, antes dos computadores, o conceito de privacidade, com o citado artigo de Warren e Brandeis. Com o advento informático, o Subcomité de Direitos Constitucionais do Senado decidiu focar-se na exploração da privacidade e no tratamento automatizado de informação, tendo sido adotados os “*Fair Information Principles*” e, em 1974, o “*Privacy Act*”.

Tendo, desta forma, o conceito de privacidade uma preocupação substantiva com o tratamento da informação sobre indivíduos, a privacidade foi redefinida como privacidade informacional, uma noção moderna, que pode ser definida como “controlo sobre as informações pessoais”, a qual conduz ao atual direito à proteção de dados pessoais ou direito à autodeterminação informacional.¹⁰⁷

A Europa prefere lidar as com questões da privacidade *online* através do paradigma de proteção de dados, enquanto os EUA utilizam leis de proteção do consumidor.¹⁰⁸

A disseminação de normas reguladoras de tratamento de dados teve lugar nos anos 80, altura em que as organizações internacionais começaram a adotar instrumentos internacionais relativos a esta temática.

No que toca ao plano europeu, o enquadramento legal de direitos humanos tem

¹⁰⁵ FUSTER, Gloria – *Op. cit.*, 2014, p. 23.

¹⁰⁶ *Ibidem*, p. 27.

¹⁰⁷ *Ibidem*, p. 48.

¹⁰⁸ WITZLEB, Normann *Et Al* – *Op. cit.*, 2014, p. 24.

sido desenvolvido para providenciar o mais alto nível de proteção à privacidade e à proteção de dados.¹⁰⁹

A substância das normas europeias é, certamente e, em larga medida, comparável à privacidade informacional dos EUA. Mas, existe quem considere que a proteção da privacidade é uma maior prioridade na Europa do que nos EUA.¹¹⁰

Os regimes europeus de proteção da privacidade dos dados desenvolveram-se como resposta às limitações ao direito à vida privada, consagrado no art. 8.º da CEDH, de modo a lidar com o tratamento automatizado de dados pessoais de larga escala dos anos 70.

No início dos anos 70 foi defendido que, com o advento dos computadores, o art. 8.º da CEDH não oferecia proteção suficiente aos indivíduos. Porém, com o desenvolvimento da jurisprudência do TEDH, a qual alargou o âmbito do referido artigo, na década seguinte, foi alegado que este era suficientemente efetivo para uma proteção satisfatória e, por isso, seria desnecessário um direito adicional, sendo este artigo também relevante para a proteção de dados.

Existe a ideia de que a CEDH é um instrumento vivo que deve ser interpretado de acordo com as condições presentes, o que constitui uma característica central da jurisprudência do Tribunal. Estas considerações importam devido à relação próxima entre os sistemas de direitos fundamentais da UE e da CEDH, desempenhando as decisões do TEDH um papel vital.¹¹¹

A Diretiva da UE não acolhe formalmente as noções de “proteção de dados pessoais”, mas descreve como um dos seus objetivos obrigar os Estados-Membros a proteger os direitos e liberdades das pessoas e, em particular, o direito à privacidade.

Para justificar uma alusão ao direito de proteção de dados pessoais, tem sido arguido que este adquiriu significado autónomo ao longo dos últimos 30 anos, através da

¹⁰⁹ *Ibidem*, p. 4.

¹¹⁰ SHAPIRO, Andrew L. – *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*. Nova Iorque: PublicAffairs, 1999. P. 164.

¹¹¹ FINK, Udo – *Op. cit.*, 2014, Pp. 90-91.

jurisprudência do TEDH e da CDFUE.¹¹²

A nível nacional, a doutrina autonomizou um direito especial de personalidade referente à defesa da intimidade da vida privada. Este direito constitui um direito fundamental e um direito de personalidade ligado estreita, direta e incindivelmente à pessoa e ao qual se contrapõe, desta forma, uma obrigação geral de respeito. A tutela da privacidade ou da “vida privada”, na expressão da lei, deverá ser definida por oposição ao conceito de vida pública.¹¹³

Assim, o direito à autodeterminação informativa nasce para garantir um direito à intimidade privada no que ao tratamento de dados diz respeito.¹¹⁴

Por último e mais concretamente, analisar-se a adequação do paradigma tradicional de lei de proteção da privacidade a lidar com os desafios da Internet.

Primeiro, quanto ao grau no qual a terminologia de privacidade de dados se traduz para a *Internet*, pode afirmar-se que os termos tecnologicamente neutrais das leis de privacidade se encontram a um nível suficientemente geral para se aplicar a plataformas baseadas na *Internet*. Um problema consiste na extensão na qual as ações *online* de indivíduos privados e as interações em serviços de redes sociais se incluem na exceção para “atividades pessoais ou domésticas”, de acordo com a al. c) do n.º 2 do art. 2.º do Regulamento Geral e na questão de se a informação que é globalmente acessível está sujeita a regras de transferências transfronteiriça de dados.¹¹⁵

Deve ter-se em consideração os desafios que a *Internet* coloca ao paradigma da privacidade dos dados. De uma perspetiva de lei e regulação, a *Internet* é inerentemente transgressiva: é global, radicalmente descentralizada e um caos em termos de governação. Os princípios essenciais das regras de privacidade de dados

¹¹² FUSTER, Gloria – *Op. cit.*, 2014, p. 91.

¹¹³ Moniz, Helena – *Op. cit.*, 1997, pp. 235-237.

¹¹⁴ CASTRO, Catarina Sarmento – *Op. cit.*, 2005, pp. 24-25.

¹¹⁵ BYGRAVE, Lee A. – Data privacy law and the *Internet*: policy challenges. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 259-289. P. 264 e ss.

são, em larga medida, incompatíveis com a lógica “aberta” da *Internet*. É importante evitar uma regulação excessiva, pois esta poderia asfixiar o potencial aberto da *Internet* de gerar inovação ou poderia ser inexecutável na prática.¹¹⁶

4.1.2. Distinção entre direito à privacidade e direito à proteção de dados

A CDFUE, proclamada como declaração política em 2000, reconheceu o direito à proteção de dados, mas o seu Memorando Explicativo não explicita o motivo da adição deste ao pré-existente direito à privacidade, nem esclarece de que modo devem os dois direitos interagir.¹¹⁷

Uma explicação avançada por diversos autores para a introdução do direito à proteção de dados na Carta prende-se com o objetivo de reforço da legitimidade do enquadramento da proteção de dados da UE através da ênfase da dimensão de direito fundamental da Diretiva.¹¹⁸

Porém, parece descabido ser necessário reconhecer um novo direito para providenciar *ex post* legitimidade à legislação existente.

Outra possível explicação é a de que a introdução desse direito estende a aplicação dos princípios essenciais de lei de proteção de dados a tratamentos de dados em áreas anteriormente abrigadas pelos segundo e terceiro pilares da UE. Assim, o direito à proteção de dados poria fim aos diferentes regimes aplicáveis.

Contudo, este direito parece improvável a exercer esse papel, uma vez que o Tratado de Lisboa acabou com a estrutura de pilares e conferiu uma base legal para

¹¹⁶ *Ibidem*, pp. 280 e ss.

¹¹⁷ LYNKEY, Orla, *Op. cit.*, 2015, pp. 89-90.

¹¹⁸ HERT, Paul de e GUTWIRTH, Serge – Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, S., POULLET, Y., HERT, P., TERWANGNE, C. e NOUWT, S. (Ed.) - **Reinventing Data Protection**, Cap. 1. Heidelberg: Springer, 2009. P. 9.

a legislação de proteção de dados, cobrindo todos os aspetos do Direito da UE.¹¹⁹

Assim, podemos considerar que a inclusão deste novo direito na Carta reflete a sua autonomização como Direito Fundamental diferente do direito à privacidade.

Porém, surge a dúvida relativa à distinção entre o direito à privacidade e o direito à proteção de dados. Assinalam-se, assim, as três doutrinas existentes a este respeito, seguindo a divisão doutrinária defendida por Orla Lynskey.

Assim sendo, a ligação entre os dois direitos pode ser concetualizada, de forma ampla, de três modos: estes direitos existem separadamente, mas são complementares; o direito à proteção de dados constitui uma subcategoria do direito à privacidade; e o direito à proteção de dados consiste num direito independente que serve uma multiplicidade de funções, incluindo a proteção da privacidade, mas não se limitando a esta.¹²⁰

No **1.º modelo**, o direito à proteção de dados e o direito à privacidade são considerados ferramentas complementares que servem para assegurar o respeito pela dignidade humana, uma vez que o Direito deve regular a atividade de todos os que tratam dados pessoais, diretamente respeitantes à pessoa.

Além disso, o TJ tem incorporado o direito à dignidade humana na ordem jurídica da UE e pode invocá-la aquando da interpretação de normas de proteção de dados, até porque este é um valor universal e indivisível, tal como consagrado no art. 1.º da Carta.

Considera-se, assim, que o princípio da dignidade da pessoa humana providencia a base concetual do direito à proteção de dados. Este seria também sustentado pelo direito à autodeterminação informacional, tal como foi defendido pelo *Bundesverfassungsgericht*, o Tribunal Constitucional Federal da Alemanha, na sua decisão de 1984, relativa ao caso “*The Population Census Decision*”. Esta decisão diz respeito a um recenseamento populacional levado a cabo pelo governo federal alemão em 1983 e que suscitou, por parte da população, medo de vigilância e um

¹¹⁹ LYNSKEY, Orla, *Op. cit.*, 2015, p. 92.

¹²⁰ *Ibidem*, p. 90.

sentimento de que este censo estatístico constituiria uma injusta invasão da privacidade. Esta questão foi levada até ao Tribunal Constitucional Federal, o qual decidiu que o referido censo era parcialmente inconstitucional, tendo sido, por isso, anulado. Como base desta decisão, o Tribunal apoiou-se num novo direito básico, o direito à autodeterminação informacional, que seria a âncora legal da proteção de dados.¹²¹

Este novo direito significaria que cada um pode determinar pessoalmente como e em que medida se deve comunicar informações sobre si a terceiros. Este direito fundamental e os seus corolários constituem o que se pode designar como os direitos individuais face à informatização dos dados.¹²²

Este modelo apresenta algumas debilidades, entre as quais se aponta o facto de alguns direitos da legislação de proteção de dados parecerem justificar-se por preocupações de dignidade humana, como é o caso do direito de acesso, mas outros são mais difíceis de se basear neste valor, como o direito à portabilidade.

Não obstante o princípio da dignidade humana ser uma justificação filosófica para os direitos fundamentais em inúmeros ordenamentos jurídicos, existe pouco consenso relativamente ao seu conteúdo preciso. E, sem existir uma tradição constitucional comum, seria contra a abordagem do TEDH a utilização de discricionariedade na aplicação deste direito.¹²³

Outras objeções a este modelo dizem respeito ao facto de o princípio da dignidade humana se encontrar no Capítulo sobre a Dignidade da Carta, enquanto o direito à proteção de dados se inclui no Capítulo das Liberdades. E, sendo o direito da dignidade humana um direito inviolável, contrasta com o objetivo do regime de proteção de dados em facilitar o livre movimento de dados.

¹²¹ HORNUNG, Gerrit e SCHNABEL, Christoph – Data protection in Germany I: The population census decision and the right to informational self-determination. *In: Computer Law & Security Report*, Vol. 25, Issue 1, 2009, pp. 84-88. P. 84.

¹²² MONIZ, Helena – *Op. cit.*, 1997, pp. 251-252.

¹²³ LYNSKEY, Orla, *Op. cit.*, 2015, p. 99.

No **2.º modelo**, o direito à proteção de dados é considerado uma mera faceta mais atual do direito à privacidade. Alguns Estados consideram, assim, o primeiro como subcategoria do direito à privacidade, nomeadamente Espanha e a Finlândia. Deste modo, o direito à privacidade, inicialmente concetualizado como o direito à “não ingerência na vida privada” ou “direito a estar sozinho”, teria evoluído de modo a incluir elementos de controlo informacional. De acordo com este modelo, todos os elementos do direito à proteção de dados são justificados por preocupações de privacidade.

Porém, pode questionar-se qual a relação do direito à proteção de dados com outros elementos que constituem o direito à privacidade e qual o seu denominador comum.

Por fim, em conformidade com o **3.º modelo**, o direito à proteção de dados serve diversos propósitos, sendo um deles relativo a fins de privacidade, mas não lhe é limitado. Poucas manifestações diretas de conceções orientadas para a intimidade da privacidade podem ser encontradas nas regras de proteção de dados e, além disso, os conceitos mais amplos da privacidade não explicam os princípios da proteção de dados.¹²⁴ É indiscutível que o direito à proteção de dados se sobrepõe, consideravelmente, ao direito à privacidade, dado que ambos visam assegurar a privacidade informacional, contudo, o primeiro serve um número de finalidade que a privacidade não prossegue e vice-versa, como referido no Relatório Rand, de 2009¹²⁵.

Da mesma forma, o direito à proteção de dados confere aos indivíduos mais direitos sobre um maior leque de tipos de informação do que o direito à privacidade quando aplicado ao tratamento de dados pessoais, uma vez que oferece controlo reforçado sobre os dados.

¹²⁴ HERT, Paul e GUTWIRTH, Serge – *Op. cit.*, 2009, p. 8.

¹²⁵ ROBINSON, Neil, GRAUX, Hans, BOTTERMAN, Maarten e VALERI, Lorenzo - Review of the European Data Protection Directive. Cambridge: Rand Corporation, 2009. P. 7.

Este Relatório é efetuado pela empresa RAND Europe, um instituto de pesquisa independente, contratada para ajudar na tomada de decisões e na definição de políticas sobre variadas áreas.

Porém, nenhum dos referidos modelos contém uma explicação definitiva sobre a interação do direito à proteção de dados com o direito à privacidade.

Ao longo dos anos 90, a “privacidade” foi utilizada na UE em relação à proteção de dados pessoais e no campo das comunicações eletrónicas, como se comprova na Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações¹²⁶.

Esta última foi substituída pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas¹²⁷, na qual se estendeu a proteção aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas.

De modo a justificar a alusão ao direito de proteção de dados pessoais, tem sido arguido que este direito adquiriu um significado autónomo através da jurisprudência do TEDH e da CDFUE, o que não é aceite por vários Estados.¹²⁸

Para além da distinção entre ambos os conceitos, pode, ainda, proceder-se a uma diferenciação no tocante à legislação de proteção de dados e à de privacidade. Assim, estas podem distinguir-se com base em quatro fatores de ordem. O primeiro elemento de distinção concerne à natureza das partes às quais se aplicam. Assim, as regras da CEDH, que protegem o direito à privacidade, apenas podem ser invocadas contra entidades públicas, enquanto as regras europeias de proteção de dados têm maior âmbito de aplicação pessoal, sendo igualmente aplicáveis a partes públicas ou privadas. O segundo diferencial respeita ao leque de dados que protegem, e, assim sendo, a legislação de proteção de dados da UE aplica-se a dados pessoais, um

¹²⁶ Transposição para a ordem jurídica portuguesa através da Lei n.º 69/98 de 28/10/1998, publicado no Diário da República, 1.ª série A, n.º 249, de 1998-10-28, p. 5572.

¹²⁷ Transposição por Decreto-Lei n.º 7/2004, publicado no Diário da República, 1.ª série A, n.º 5, de 2004-01-07, p. 70.

¹²⁸ Veja-se o caso do Direito Alemão, no qual se considera que o direito à proteção de dados é derivado do direito à privacidade.

termo amplamente definido pelo legislador, e, apesar da expansiva interpretação do TEDH relativamente ao direito à privacidade, é frequentemente defendido que este não se aplica ao mesmo amplo leque de situações. Em terceiro lugar, a diferença entre ambas as legislações pode aferir-se através das atividades a que se estendem, visto que o regime de proteção de dados se aplica a todas as formas de tratamento, sendo por isso aplicáveis a mais largo leque de atividades relacionadas com dados do que o direito à privacidade. Finalmente, a quarta causa de distinção diz respeito aos direitos conferidos aos indivíduos, quanto aos quais o art. 8.º da CEDH confere um mais limitado leque de direitos de informação do que a legislação europeia de proteção de dados.¹²⁹

Porém, mantém-se a dúvida sobre qual a verdadeira relação entre o direito à privacidade e o direito à proteção de dados.

No caso *Promusicae*, de 2008, o TJ incorporou a análise da proteção de dados na sua decisão e referiu-se-lhe como “direito fundamental” pela primeira vez. Porém, esta referência supôs que o direito à proteção de dados é uma categoria do direito à privacidade, apesar de o Tribunal reconhecer que estes direitos foram reconhecidos de forma independente na Carta.

Esta amálgama de direitos subsistiu, mesmo após a aquisição de força vinculativa pela Carta, em 2009. Porém, os direitos são distintos, na opinião de diversos autores e, em variados casos que correm os seus termos no TJ, são invocados como dois direitos diferentes. Assim, “(...) *um direito clássico (a proteção da vida privada ao abrigo do artigo 8.º da CEDH) e um direito mais moderno (as disposições da Convenção n.º 108 em matéria de proteção dos dados). A Carta consagra direitos semelhantes, respetivamente, nos seus artigos 7.º e 8.º. O Tribunal de Justiça reconheceu já a estreita ligação entre os direitos fundamentais ao respeito pela vida privada e à proteção dos dados*”.¹³⁰

No Acórdão *Google Spain*, de 13 de maio de 2014, o TJ menciona o direito à proteção

¹²⁹ LYNKEY, Orla, *Op. cit.*, 2015, pp. 112-127.

¹³⁰ Ponto 71 das Conclusões da Advogada-Geral Eleanor Sharpston apresentadas em 17 de junho de 2010, no âmbito do Acórdão *Schecke E Eijfert*, relativo aos Processos Apensos C-92/09 E C-93/09.

de dados como um “direito à vida privada, no que diz respeito ao tratamento de dados pessoais”, referindo-se-lhes como um só direito.¹³¹

Resta a dúvida de se o Tribunal encara, efetivamente, a proteção de dados como uma categoria do direito à privacidade, ou se ainda não foi conferida explícita atenção a esta questão.

Apesar de todas as incertezas, avança-se no sentido de um verdadeiro direito de controlo de dados pessoais, que se inclui no direito à proteção de dados pessoais.

Este controlo individual tem dois papéis: um concetual, enquanto base do regime, e um instrumental, que influencia a forma como os direitos-chave da proteção de dados são interpretados. Ambos os papéis se encontram interligados, ou seja, se for aceite que o controlo deve ser uma faceta da proteção de dados, então esta noção pode influenciar a forma como os conceitos são interpretados e aplicados.¹³²

O controlo é um pré-requisito para a habilidade individual de auto-apresentação, crucial para o livre desenvolvimento da personalidade individual. Pode ajudar a minimizar o efeito inibidor da “*dataveillance*”, isto é, da prática de monitorizar e coletar dados *online* e o impacto negativo que o efeito controlador da vigilância pode ter na autonomia individual.

O controlo individual deve funcionar como configuração padrão na lei de proteção de dados da UE, ou seja, a legislação deve ser interpretada e aplicada de modo a maximizar o controlo, contudo tal controlo não deve ser absoluto e pode ser revogado. Enfrenta, porém, vários obstáculos práticos e, por isso, deve ser reforçado por garantias estruturais.

4.1.4. Posição adotada

Enquanto o direito à privacidade tem sido formulado num sentido negativo, como uma liberdade, o direito à proteção de dados pessoais, na UE, constitui um direito

¹³¹ Acórdão *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, relativo ao Processo C-131/12.

¹³² LYNKEY, Orla, *Op. cit.*, 2015, pp. 227-228.

em sentido positivo, um direito quanto ao qual se espera que a informação sobre a pessoa seja tratada de forma respeitosa e que esta a possa controlar de modo efetivo.

A CDFUE, em 2000, consagrou, no art. 8.º, pela primeira vez na história, a proteção de dados pessoais como um direito fundamental independente e, por isso, mais do que um aspeto do direito geral à privacidade, o qual se encontra separadamente regulado no art. 7.º.

Existem elementos da proteção de dados que não se encaixariam na privacidade, e deve lembrar-se que a CEDH é um produto do seu tempo, tendo sido promulgada em 1950, e que, por isso, é normal que não contenha nenhuma regra específica relativa ao tratamento digital de dados pessoais.

O direito à proteção de dados vai além de meramente modernizar o direito à privacidade e o trazer para a idade digital. Procura proteger diferentes interesses individuais de controlar a manipulação de informação pessoal, proteção essa que supera a mera proteção da privacidade e que é melhor concebida como um direito pró-ativo a gerir os próprios dados pessoais face à quantidade de pressão tecnológica sobre tal controlo.

O conteúdo e a natureza do direito de proteção de dados continuam sem se entender na sua totalidade, o que coloca em perigo o seu potencial na ordem jurídica da UE, porém o mesmo encontra-se explicitamente consagrado.

Apesar de fortemente sobrepostos, estes direitos são distintos e o terceiro modelo apresentado parece ser o que melhor reflete esta relação. Esta distinção releva, uma vez que o TJ já por diversas vezes mesclou ambos os direitos, interpretando, muitas vezes erradamente, o direito à proteção de dados.

Este modelo parece ser o que mais respeita as tradições constitucionais divergentes dos Estados-Membros e o que mais segue a interpretação do direito à privacidade do TEDH, uma vez que nem todos os elementos da proteção de dados caem no âmbito da privacidade.

4.2. Conceito e categorias de dados pessoais

Deve, agora, definir-se o conceito de “dados pessoais” e distinguir entre as suas diversas categorias.

Deve-se, antes de mais, explicitar que quem pode usufruir das vantagens inerentes a estas posições jurídicas são os denominados “titulares” e os que estão vinculados ao seu cumprimento são as “as entidades a quem elas se destinam”¹³³, ou os “responsáveis pelo tratamento”.

4.2.1. Noção de dados pessoais

A informação representa poder e a posse de informações significa disposição de poder sobre a pessoa. O poder torna-se maior quanto mais tais informações forem múltiplas e diferenciadas.¹³⁴

Uma certa informação pode conter um vínculo objetivo a uma determinada pessoa, revelando algo sobre a mesma e, nesse caso, o objeto dessa informação é a própria pessoa, tornando-a em informação pessoal.

Há autores que clarificam e defendem que o que se pretende proteger são as pessoas e não os dados.¹³⁵

Um “dado” é informação em estado potencial, uma espécie de “pré-informação”, antes da interpretação. “Informação” alude a algo além da representação contida no dado. A informação pessoal está ligada à privacidade: maior grau de privacidade equivale a menor difusão de informações pessoais e vice-versa.¹³⁶

O enunciado linguístico “dados” é o plural da expressão latina *datum* e está utilizada no sentido que hoje lhe empresta a ciência informática: representação convencional

¹³³ GOUVEIA, Jorge Bacelar – *Op. cit.*, 1991, p. 709.

¹³⁴ SILVEIRA, Luís Lingnau da - A Protecção de dados pessoais na *Internet*. In: **Europa: Novas Fronteiras**, n.º 28-29, janeiro/dezembro 2011, pp. 139–143. Pp. 141-142.

¹³⁵ MONIZ, Helena – *Op. cit.*, 1997, p. 240.

¹³⁶ DONEDA, Danilo - *Op. cit.*, 2011, p. 94.

de informação, sob a forma analógica ou digital, possibilitadora do seu tratamento automático.¹³⁷

A definição de “dados pessoais” constante da alínea a) do art. 2.º da Diretiva 95/46/CE, ao delimitá-los como “(...) *qualquer informação relativa a uma pessoa singular identificada ou identificável (« pessoa em causa »); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*”, vai além da definição da Convenção n.º 108, que se reduz, na terminologia da Diretiva, à “identificação da pessoa em causa”. A técnica consiste em definir dados pessoais com recurso à qualificação dos titulares. A expressão “*informação relativa a*”, associada a elementos específicos de identidade, permite a relação da definição com aspetos da personalidade do titular que revestem um carácter de não imediata identificação, de subjetividade ou mesmo de erro ou incompletude.¹³⁸

A qualificação como “dato pessoal” está, assim, sujeita a um princípio de reconhecimento, isto é, é necessário que a pessoa seja identificável. O considerando 26.º da Diretiva menciona a anonimização como delimitação negativa do âmbito da mesma, ao referir “(...) *que os princípios da protecção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável (...)*”.

Porém, no processo de tratamento de dados pessoais é necessária alguma identificação para garantir a eficácia e prossecução das finalidades das operações.

¹³⁷ CANOTILHO, Gomes e MOREIRA, Vital – *Op. cit.*, 2007, p. 550.

¹³⁸ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 643.

Aliás, na Sociedade da Informação, o papel dos dados pessoais pode ser comparado com o desempenhado pelo petróleo na sociedade industrial.¹³⁹

Apesar de alguns autores considerarem que, constituindo a identidade ou identificabilidade da pessoa um elemento caracterizador do dado como pessoal, não estamos perante um dado pessoal para efeitos da lei quando os elementos constantes do dado, apesar de relativos à pessoa, não permitirem o seu reconhecimento¹⁴⁰, outros há que consideram que, não obstante este conceito amplo, não parece que a sua funcionalização à identificação ou identificabilidade esgote a *ratio* do texto. Ou seja, há dados que não permitem identificar o titular, mas permitem admitir a sua existência¹⁴¹.

Na alínea 1) do art. 4.º do Regulamento Geral, a definição de “dados pessoais” mantém-se, praticamente, inalterada, considerando-se como “dados pessoais” a “(...) *informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.*”.

No caso *Kbelili*, de 2011, o TEDH considerou que, para determinar se os dados pessoais envolvem a vida privada, é preciso considerar o contexto em que os mesmos foram recolhidos e armazenados, a sua natureza, a forma como foram usados e tratados e os resultados que se pode obter pelo seu tratamento.¹⁴²

No âmbito nacional, também a alínea a) do art. 3.º da Lei n.º 67/98, de 26 de outubro, que transpõe a mesma Diretiva, mantém a definição, acrescentando

¹³⁹ BLUME, Peter – Is it Time for Tomorrow: EU Data Protection Reform and the *Internet*. In: **Journal of Internet Law**, Vol. 18, n.º 8, 2015, p. 3-13. P. 4.

¹⁴⁰ MONIZ, Helena – *Op. cit.*, 1997, p. 242.

¹⁴¹ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 645.

¹⁴² FUSTER, Gloria – *Op. cit.*, 2014, p. 100.

apenas, que é “dado pessoal” toda a informação daquele tipo independentemente do seu suporte. Assinala-se que esta Lei se aplica, de acordo com o art. 4.º, ao “(...) *tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados (...)*”.

4.2.2. Diferentes categorias de dados pessoais

Os dados pessoais têm vários degraus de sensibilidade.¹⁴³

Existem diversas categorias de dados pessoais e podemos distinguir entre dados não sensíveis (os denominados, simplesmente, “dados pessoais”, que incluem informações relativas à data de nascimento e ao estado civil, por exemplo) e dados sensíveis (como a situação patrimonial e financeira e o estado de saúde), sobre os quais é proibido o tratamento.

A doutrina costuma distinguir três esferas na defesa da privacidade, sendo elas a pública, a privada (relativa a dados não sensíveis) e a íntima (que diz respeito a dados sensíveis). Porém, deve sempre lembrar-se que a reserva da privacidade deve ser considerada a regra e não a exceção.¹⁴⁴

Existe uma proibição geral de tratamento de dados que revestem uma especial sensibilidade, a qual encontra fundamento jurídico tanto, a nível da UE, no art. 8.º da Diretiva 95/46/CE e no art. 9.º do Regulamento Geral, como, a nível nacional, no n.º 3 do art. 35.º da CRP e no art. 7.º da LPD. Os citados instrumentos de Direito da UE não referem no elenco de proibições de tratamento, a ideia de “vida privada”, a qual existe na LPD devido à CRP, como nota Catarina Sarmiento e Castro.¹⁴⁵

¹⁴³ LINDSAY, David – *Op. cit.*, 2014, p. 299.

¹⁴⁴ VASCONCELOS, Pedro Pais de - Protecção de Dados Pessoais e Direito à Privacidade. *In: Direito da Sociedade da Informação*, Vol. I. Coimbra: Coimbra Editora, 1999, pp. 241–253. P. 250.

¹⁴⁵ *Ibidem*, p. 96.

A nível nacional, uma parte da doutrina portuguesa distingue três esferas: a esfera privada, que respeita a aspetos não públicos, mas que não podem ser pessoais; a esfera pessoal, que, sendo mais restrita, abarca aspetos ligados à própria pessoa; e a esfera de segredo, na qual cabem coisas naturalmente secretas, mas que podem não ser pessoais.¹⁴⁶

O regime estabelecido para a proteção de tratamento automatizado de dados pessoais funciona como garantia do direito à proteção da vida privada ou à proteção da intimidade da vida privada, estabelecendo o n.º 2 do art. 35.º da CRP uma garantia do direito à reserva da vida privada (protegendo, assim, os dados pessoais) e o n.º 3 do mesmo artigo, uma garantia do direito à reserva da intimidade da vida privada (referente aos dados sensíveis).¹⁴⁷

Podemos concluir que o regime referente ao tratamento de dados pessoais pretende proteger o direito à reserva da vida privada em sentido amplo e afirmar outro direito fundamental, o direito à autodeterminação informacional.

Assim, “*contrapondo-se à ideia de arcana praxis, tende hoje a ganhar contornos um direito geral à autodeterminação informativa que se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização dos seus dados pessoais*”.¹⁴⁸

4.2.3. Conceito de tratamento de dados pessoais

A criação e a manutenção de um conjunto estruturado de dados pessoais podem acarretar perigos para os titulares dos dados e constituem, por isso, tarefas de responsabilidade, em que existe sujeição a obrigações de cujo incumprimento resultam sanções. É necessário, assim, regular o tratamento de dados pessoais.¹⁴⁹

¹⁴⁶ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, pp. 22-24.

¹⁴⁷ MONIZ, Helena – *Op. cit.*, 1997, p. 246.

¹⁴⁸ CANOTILHO, José Joaquim Gomes – *Direito Constitucional e Teoria da Constituição*, 7.^a edição (10.º reimpressão). Coimbra: Almedina, 2003. P. 515.

¹⁴⁹ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, p. 65.

Há necessidade do binómio nome-identificação no processo de tratamento de dados pessoais e, desta forma, a identificabilidade é necessária para garantir a eficácia e a prossecução das finalidades das operações.¹⁵⁰

No direito à proteção de dados da UE, a legitimidade do tratamento de dados não é assumida, deve ser assegurada pelo responsável. Ou seja, não se considera aceitável o tratamento *per se*, devendo o responsável pelo mesmo demonstrar que reúne as condições de legitimidade necessárias para efetuar esse tratamento.¹⁵¹

Por vezes, os dados pessoais provocam disputas. Existem empresas que se dedicam exclusivamente a tratar dados pessoais e se uma outra empresa, tal como uma empresa encarregue de uma rede social, lhes recusa o tratamento dos dados que nela circulam, pode levar estas últimas a dispor livremente de investimentos rivais e a manter monopólios através da exclusão de concorrentes.¹⁵² Esta situação comprova a delicadeza dos assuntos relacionados com a proteção e o tratamento dos dados.

As regras sobre tratamento de informação surgiram na Europa nos anos 70, na Alemanha Federal, na Suíça e em França e tinham como objetivo servir a privacidade.¹⁵³

Tendo em conta que toda a Diretiva 95/46/CE é construída em torno do conceito de “tratamento de dados pessoais”, a sua definição, exposta na al. b) do art. 2.º, alarga a área de proteção, abrangendo “(...) *qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados* (...)”. Também da al. b) do art. 3.º da LPD consta a mesma noção. Ambos os documentos excluem do seu âmbito de aplicação, porém, o tratamento de dados pessoais efetuado por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, por

¹⁵⁰ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 644.

¹⁵¹ HUSTINX, Peter – “Ensuring more effective data protection in an age of big data”. Contribuição para “*European Voice online debate on big data and consent*”, 2014.

¹⁵² Citando o caso *PeopleBrowsr v. Twitter*, ver ABRAHAMSON, Zachary - Essential Data. In: **The Yale Law Journal**, Vol. 124, 2014, pp. 867–881. Pp. 867-868.

¹⁵³ FUSTER, Gloria – *Op. cit.*, 2014, p. 21.

exemplo na correspondência ou em listas de endereços, como é referido no n.º 2 do art. 3.º da Diretiva e no n.º 2 do art. 4.º da Lei.

Também com o novo Regulamento esta definição é preservada, referindo-se, na al. 2) do art. 4.º, como “tratamento de dados pessoais” “(...) *uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*”.

A regra-chave relativa ao tratamento de dados pessoais é que este apenas pode ocorrer quando exista uma condição de legitimidade que o fundamente, tal como estabelecido pelo art. 6.º do Regulamento. Quando preenchido qualquer um dos requisitos enumerados, terão de ser cumpridos os princípios gerais de proteção.

O principal modo de legitimar este tratamento consiste no “consentimento”, o qual se encontra previsto na al. a) do n.º 1 do citado artigo. Este constitui o fundamento geral e mais abrangente do tratamento. Mas, mesmo que o fundamento habilitante seja o consentimento, se os dados tratados não cumprirem os requisitos de qualidade, o seu tratamento será ilegítimo.¹⁵⁴

Este consentimento da parte do titular dos dados deve ser uma manifestação de vontade livre, ou seja, sem qualquer pressão ou restrição e sem que o titular sofra consequências; específica, isto é, conferida em função de um certo período temporal restrito e para uma finalidade e circunstância conhecida antecipadamente; e informada, em relação à finalidade e à extensão exata do consentimento.¹⁵⁵

Alguns autores consideram que a Diretiva e a Lei se basearam numa certa administrativização da matéria, com frequente subordinação a autorizações administrativas e com conceitos-base fixados com muita amplitude, o que conduz a

¹⁵⁴ O que nos recorda a suprarreferida “questão do duplo teste”. Ver: CASTRO, Catarina Sarmento – *Op. cit.*, 2005, p. 205.

¹⁵⁵ *Ibidem*, pp. 206-207.

que o fundamento da defesa da personalidade se dilua no complexo de regras formais acumuladas. Assim, a lei peca por excesso, aplicando-se a simples atividades normais, e por defeito, visto que as particularidades da intromissão informática acabam por não ser atendidas.¹⁵⁶

Deve considerar-se que os utilizadores da *Internet* e os serviços de redes sociais, por exemplo, partilham uma responsabilidade conjunta pelo tratamento de dados pessoais enquanto “responsáveis pelo tratamento” nas aceções da al. d) do art. 2.º, da Diretiva, e da al. 7) do art. 4.º do Regulamento, se bem que em diferentes graus e com tipos de obrigações diferentes.¹⁵⁷

Apesar de o TEDH nunca ter declarado qualquer tratamento de dados pessoais como uma ingerência nos direitos do art. 8.º da CEDH, decidiu que o seria a recusa de garantir aos indivíduos acesso à informação.¹⁵⁸

É importante referir, neste contexto, e a propósito do tratamento de dados pessoais através da *Internet*, que esta noção tem consequências bastante amplas no mundo virtual, devendo ter-se em conta, nomeadamente, o Acórdão *Lindqvist* do TJ¹⁵⁹, em 2003, no qual foi declarado que a operação que consiste na referência, feita numa página da *Internet*, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um “tratamento de dados pessoais por meios total ou parcialmente automatizados” na aceção do n.º 1 do art. 3.º da Diretiva.

¹⁵⁶ ASCENSÃO, José de Oliveira – *Op. cit.*, 2001, pp. 211-212.

¹⁵⁷ HUNSTINX, Peter - Parecer da AEPD sobre a promoção da confiança na sociedade da informação através do reforço da protecção dos dados e da privacidade, n.º2010/C280/01, de 16 de outubro de 2010, ponto 74.

¹⁵⁸ FUSTER, Gloria – *Op. cit.*, 2014, p. 102.

¹⁵⁹ Acórdão *Lindqvist*, de 6 de novembro de 2003, no âmbito do Processo C-101/01.

Atualmente, parte da recolha de dados através da *Internet* ocorre em virtude de tratamentos de dados pessoais que têm como responsável um órgão de pessoa coletiva da AP.¹⁶⁰

Como realça Catarina Sarmiento e Castro, “(...) *ao tratamento de dados pessoais recolhidos na Internet aplicam-se as regras gerais de protecção de dados*”, existindo, contudo, regras que têm em linha de conta, concretamente, as redes abertas, como é o caso do n.º 4 do art. 10.º da LPD.¹⁶¹

A definição de tratamento de dados pessoais pode considerar-se tecnologicamente neutral, sendo este regime aplicável a tratamentos realizados através de qualquer tipo de tecnologia.

Relativamente ao tratamento, o princípio essencial é o da informação dos titulares dos dados, ou seja, os sujeitos devem ser previamente informados pelos responsáveis dessas operações acerca do teor das mesmas e das suas finalidades. Desta forma, podem opor-se ou consentir no tratamento dos seus dados, conforme considerem mais ajustado aos seus interesses.¹⁶²

Apesar de a *Internet* perturbar e transformar as normas do comportamento humano, Giovanni Buttarelli, atual AEPD, considera um “disparate” afirmar que, na era digital, a privacidade morreu. Isto porque não há provas de que a *Internet* distorça fundamentalmente os nossos valores enquanto sociedade.¹⁶³

Existem quatro linhas de abordagem ética quando se trata do direito à proteção de dados¹⁶⁴:

¹⁶⁰ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005. P. 166

¹⁶¹ *Ibidem*, pp. 162-163.

¹⁶² SILVEIRA, Luís Lingnau da – *Op. cit.*, 2011, pp. 141-142.

¹⁶³ BUTTARELLI, Giovanni – “Ethics at the Root of Privacy and as the Future of Data Protection”. Discurso em “*Berkman Center for Internet and Society at Harvard University and the MIT Internet Policy Initiative and the MIT Media Lab*”, 2016. P. 2.

¹⁶⁴ *Ibidem*, p. 4.

- ✚ A privacidade e a proteção de dados importam para a proteção da dignidade humana, ao permitirem aos indivíduos desenvolverem as suas personalidades e terem vidas independentes nas quais exercitem outros direitos e liberdades;
- ✚ As tecnologias não devem ditar os nossos valores e direitos;
- ✚ A adesão à lei no ambiente digital não é suficiente e deve ser conciliada com uma vertente ética do tratamento de dados pessoais; e
- ✚ O “*big data*” tem implicações filosóficas, legais e morais, as quais devem ser incluídas na nossa reflexão na sociedade digital.

4.2.4. Posição adotada

São necessários mecanismos que possibilitem à pessoa deter conhecimento e controlo sobre os seus próprios dados que, no fundo, são expressão direta da sua personalidade. Aliás, em diversos ordenamentos jurídicos, a proteção de dados pessoais é um verdadeiro direito fundamental, tal como o é na UE, por ser um instrumento considerado essencial para a proteção da pessoa e da dignidade humana, sendo-lhe, por isso, concedido um tratamento jurídico autónomo.

Desta forma, quando se concretize um dos fundamentos legitimantes de uma operação de tratamento de dados, na qual se concedem direitos aos titulares desses dados e se atribuem correspondentes obrigações aos responsáveis por esse tratamento, serão aplicáveis princípios orientadores desse tratamento, referidos adiante.

5. DIREITO À PROTEÇÃO DE DADOS PESSOAIS NO REGULAMENTO GERAL

Após um estudo relativamente às fontes do direito à proteção de dados e, consequentemente, as que basearam o Regulamento Geral da UE, foram analisados os principais conceitos relacionados com a presente temática. Por fim, define-se, de modo mais preciso, o direito à proteção de dados pessoais de acordo com este Regulamento, com uma referência sobre a evolução deste direito até à sua concretização como um verdadeiro direito fundamental.

Seguidamente será feita uma alusão aos princípios que orientam e baseiam o tratamento de dados pessoais, e, desta forma, definem o direito à proteção de dados pessoais. Depois, será analisado o conteúdo deste último direito, mencionando-se, não só os direitos conferidos aos titulares destes dados pessoais, mas também os correspondentes deveres que concernem aos responsáveis pelo tratamento desses dados.

5.1. Evolução do direito à proteção de dados pessoais como Direito Fundamental da Diretiva 95/46/CE até ao novo Regulamento Geral da UE

A ideia de direito fundamental liga-se intrinsecamente com a dignidade humana. A amplitude e natureza destes direitos não permaneceram estáticas, foram evoluindo historicamente, enriquecendo-se com as conquistas e transformações das ideias e pensamentos da coletividade.¹⁶⁵

A necessária circulação de informação está associada ao funcionamento de um mercado interno de livre circulação de bens, pessoas, serviços e capitais, devendo, da mesma forma, assegurar-se a proteção dos direitos fundamentais das pessoas, tal como se determina no 3.º Considerando da Diretiva 95/46/CE. Para a Europa, o alto nível de proteção de dados pessoais tem sido considerado uma necessidade para garantir a confiança dos utilizadores em relação ao desenvolvimento da Sociedade da Informação.

¹⁶⁵ FARIA, Miguel José – Direitos Fundamentais e Direitos do Homem, Vol. I, 3.ª ed. revista e ampliada. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2001. Pp. 3-4.

Estando conectada com a proteção dos indivíduos, a proteção dos dados pessoais faz parte de um conjunto de valores de referência defendidos pelos países democráticos.¹⁶⁶

Importa referir que já existe uma relação próxima entre os dois sistemas de direitos fundamentais da UE e da CEDH.¹⁶⁷

Na UE, a matéria de direito à proteção de dados pessoais, tem sido regulada através da suprarreferida Diretiva 95/46/CE. Para se chegar à versão final da Diretiva, foram necessários cinco anos, porém o seu texto não considera o âmbito da *Internet* e encontra-se redigido de um modo “tecnologicamente neutral”. Na medida em que a utilização da *Internet* e a evolução da tecnologia de informação têm tomado proporções avassaladoras, o tempo no qual o texto da Diretiva se manteve inalterado constituiu um grave lapso temporal.¹⁶⁸

Assim, o regime da Diretiva foi esboçado para uma era pré-*Internet* e deve ser interpretada tendo isto presente.

A UE serviu, apesar disto, como incentivo para o resto do Mundo no que toca à adoção de regras de proteção de dados pessoais, tendo a Diretiva constituído uma medida de proteção de direitos fundamentais.

Tal como referido, inicialmente, o TJ mostrava-se constrangido por dois motivos: pelo facto de os Tratados não estabelecerem uma base legal para esta proteção e, de acordo com o princípio da atribuição, a UE não dispõe de competência geral, tendo apenas as competências que lhe foram atribuídas pelos Tratados¹⁶⁹, e por a CDFUE, que foi o primeiro instrumento a consagrar o direito à proteção de dados, ainda não

¹⁶⁶ FRAYSSINET, Jean - Is protection of Personal Data guaranteed on the *Internet*? In: CHATILLON, Georges (Ed.) - **Internet International Law: International and European Studies and Comments**. Bruxelas: Bruylant, 2005, pp. 421-429. P. 422.

¹⁶⁷ FINK, Udo – *Op. cit.*, 2014, p. 90.

¹⁶⁸ BLUME, Peter – *Op. cit.*, 2015, pp. 3-4.

¹⁶⁹ CAMPOS, João Mota, CAMPOS, João Luís Mota e PEREIRA, António Pinto – Manual de Direito Europeu. Coimbra: Coimbra Editora, 2014, 7.ª ed.. P. 278.

ter adquirido força vinculativa, o que significava que este direito não existia, efetivamente, na ordem jurídica da UE.

Contudo, dado que a falta de legislação de dados na UE seria uma ameaça ao livre movimento de dados pessoais, a Diretiva pôde, legitimamente, apoiar-se no art. 114.º do TUE, que determina sobre “*medidas relativas à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros, que tenham por objecto o estabelecimento e o funcionamento do mercado interno*”. Podemos, de qualquer forma, considerar que a Diretiva também se baseou na proteção de direitos fundamentais, uma vez que os objetivos do mercado interno e da proteção de direitos fundamentais, e, portanto, de dados pessoais são, de uma perspetiva objetiva, indissociáveis. A proteção de direitos fundamentais não foi uma mera consideração incidental aquando da adoção da Diretiva, tendo esta sido adotada tendo os objetivos de proteção de direitos fundamentais e de mercado interno como base legal.¹⁷⁰

Com o tempo, a UE foi reconhecendo os direitos fundamentais como princípios gerais de direito e, mais tarde, formulou o seu próprio catálogo, sob a forma de CDFUE. Alguns Estados só aceitaram a supremacia do Direito da UE com a condição de que este respeitaria os seus direitos fundamentais e a UE fê-lo indiretamente: não garantiu os direitos fundamentais nacionais, mas sim os direitos fundamentais da UE, os quais são, em parte, inspirados nas tradições constitucionais comuns dos Estados-Membros.¹⁷¹

Estas tradições constitucionais comuns e os direitos da CEDH foram configurados como fontes secundárias para determinar os padrões da comunidade, não como fontes diretas dos direitos fundamentais da UE.

Porém, o art. 8.º Carta não emergiu *ex nihilo*, as regras aplicáveis ao tratamento de dados estavam materializadas na maioria das fontes mencionadas, mesmo que não

¹⁷⁰ LYNKEY, Orla, *Op. cit.*, 2015, pp. 58-61.

¹⁷¹ FUSTER, Gloria – *Op. cit.*, 2014, p. 164.

na forma de direito fundamental.¹⁷² Este artigo protege, especificamente, a proteção de dados como um direito humano e restringe os Estados-Membros a recolher estes dados, tornando-se, assim, um direito qualificado.¹⁷³

A Carta indica que a Diretiva consagra um direito fundamental, pois o seu memorando explicativo refere que o direito à proteção de dados é baseado na Diretiva. Nesta perspetiva, a Carta apenas codifica o direito à proteção de dados que teve primeiramente expressão na ordem jurídica da UE através da Diretiva.

Como referido, finalmente, em 2009, o Tratado de Lisboa, forneceu uma base legal para a legislação de proteção de dados e garantiu estatuto vinculativo à Carta, reforçando significativamente as credenciais de Direitos Humanos da UE.¹⁷⁴

Em 2012, com a proposta de reforma das regras de proteção de dados da UE, a qual foi acima referida, o Novo Regulamento Geral tenta conferir aos indivíduos direitos mais efetivos, através da facilitação do seu exercício. Este Regulamento introduz novos direitos como o direito de o titular de dados a ser informado, sem demora indevidas, de uma falha de tratamento que o possa afetar a si ou à sua privacidade e o novo tipo de direito à portabilidade dos dados. O Regulamento estabelece, também, mais responsabilidade para os responsáveis pelo tratamento.

No ano de 2015, 109 países tinham já adotado legislação de proteção de dados, o que corresponde a mais de metade dos países do mundo e estes países olham para a Europa à procura de modelos, esperando pelo Regulamento Geral antes de adotarem ou reverem as suas regras.¹⁷⁵

¹⁷³ FINK, Udo – *Op. cit.*, 2014, pp. 82-88.

¹⁷⁴ LYNSKEY, Orla, *Op. cit.*, 2015, pp. 61-63.

¹⁷⁵ BUTTARELLI, Giovanni - The General Data Protection Regulation: Making the world a better place? Discurso em “*EU Data Protection 2015 Regulation Meets Innovation*”, São Francisco, 2015. P. 3.

Criou-se, assim, a esperança de que o Regulamento forneça uma equilibrada proteção de dados e contribua solidamente para a civilização da tecnologia de informação digital e para a sua principal zona de tráfego, a *Internet*.¹⁷⁶

Hoje, todos os Estados-Membros da UE têm leis de proteção de dados pessoais e estas estão, geralmente, conectadas com direitos constitucionalmente consagrados ou de importância equivalente.

Não obstante a proteção de dados ser reconhecida como um direito fundamental, tal não significa que deva prevalecer sobre outros direitos e interesses numa sociedade democrática, pelo que podem ser necessárias limitações ao exercício do mesmo. No entanto, estas limitações devem ser excecionais, devidamente justificadas e não podem afetar os elementos essenciais do próprio direito.

Porém, não é ética nem juridicamente aceitável restringir e permitir o atropelo de direitos que são ontologicamente fundantes da personalidade jurídica e da dignidade humana em homenagem a interesses comerciais e de negócios como são os da empresa ou das vendas em massa.¹⁷⁷

Quanto ao estrato nacional, o direito de proteção de dados configura um direito especial de personalidade que protege o cidadão dos perigos da informática para a sua privacidade.¹⁷⁸

O que antes era visto como uma extensão da personalidade individual, uma reserva de privacidade e uma faculdade carecida de proteção contra as tentações de interferência do poder público, foi-se construindo como um direito, fonte de obrigações específicas para os Estados e para os particulares, protegido e regulado por leis, pela ordem constitucional e por instrumentos internacionais. São os valores

¹⁷⁶ BLUME, Peter – *Op. cit.*, 2015, p. 12.

¹⁷⁷ VASCONCELOS, Pedro Pais de – *Op. cit.*, 1999, p. 249.

¹⁷⁸ CASTRO, Catarina Sarmento – *Op. cit.*, 2005, p. 32.

da privacidade, da honra, da dignidade humana, do direito ao bom nome e da liberdade individual que descrevem os condicionalismos do direito à informação.¹⁷⁹

O âmbito do que constitui “vida privada” tem vindo a mudar, constantemente, fruto dos avanços tecnológicos e das conceções sociais sobre o que constitui o “público” e o “privado”, mormente no contexto da *Internet* e das redes sociais.

A CRP criou uma série de direitos fundamentais, que cobrem praticamente todas as matérias com implicações na salvaguarda dos valores essenciais da pessoa. Esta positivação dos direitos caracteriza-se pela sua precisão e pormenorização.¹⁸⁰

A CRP consagrou um direito à autodeterminação informativa sobre a vida privada, que tutela o interesse do controlo sobre os dados pessoais. O direito à autodeterminação informativa nasce como garantia do direito à intimidade da vida privada. Assim, as normas de proteção de dados face à informática visam assegurar a reserva da vida privada e a garantia de certos direitos humanos. Atualmente, o direito à autodeterminação informativa já não é apenas um direito de garantia do direito à reserva vida privada, ou que resguarda o cidadão das intromissões não autorizadas de terceiros nas informações que lhe respeitam, num sentido de direito de defesa. É um verdadeiro direito fundamental. Constitui, hoje, um verdadeiro direito “ofensivo”, no sentido em que cada um determina o que podem os outros, a cada momento, saber a seu respeito.¹⁸¹

É uma liberdade, um poder de dispor das suas informações pessoais, de controlo para cada indivíduo preservar “a sua própria identidade informática”. Numa dimensão subjetiva, é o direito que garante ao titular posições jurídicas perante o Estado, para defesa de abusos relativos à utilização da sua informação pessoal, seja pela negativa, através da abstenção de tratamento dos dados, seja pela positiva,

¹⁷⁹ VASCONCELOS, Pedro Bacelar – Direito à Informação, Privacidade e Proteção de Dados Pessoais. In: **Fórum de Proteção de Dados**, n.º 2, 2016, pp. 8-10. P. 9.

¹⁸⁰ GOUVEIA, Jorge Bacelar – *Op. cit.*, 1991, p. 706.

¹⁸¹ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, pp. 24-29.

impondo adoção de medidas de proteção. Numa dimensão objetiva, impõe ao Estado a adoção de providências de defesa perante agressões de terceiros.¹⁸²

Podemos considerar que a proteção de dados é pensada como uma garantia, mas o seu fundamento, a autodeterminação informacional, exprime-se como uma liberdade e não esgota a complexidade da proteção de dados pessoais.¹⁸³

Quanto ao domínio da *Internet*, “A *Internet* é um caleidoscópio de regras que chocam e se contradizem”.¹⁸⁴

A Europa repetidamente considera que a proteção de dados pessoais é o “assunto-chave no desenvolvimento da Sociedade da Informação”.¹⁸⁵

A relação entre o Direito e a *Internet* pode ser encarada como o conto da relatividade de Einstein: “*Enquanto o Direito é convidado a julgar a velocidade de um comboio em andamento, está, ele próprio sentado num comboio em andamento.*”.¹⁸⁶

Em suma, a proteção de dados é considerada, pela maioria, um verdadeiro direito fundamental. Mas pode ser, ainda, encarada como um novo tipo de direito da concorrência, estimulando a cultura do cumprimento com fortes reguladores.¹⁸⁷

¹⁸² *Ibidem*, p. 28.

¹⁸³ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 806.

¹⁸⁴ CHATILLON, Georges – Presentation. *In*: CHATILLON, Georges (Ed.) - ***Internet International Law: International and European Studies and Comments***. Bruxelas: Bruylant, 2005, pp. 7-41. P. 7.

¹⁸⁵ POULLET, Yves – *Op. cit.*, 2005, pp. 124-131.

¹⁸⁶ BURKERT, Herbert - General Report Standards Applicable to the *Internet*: Benefits and Limitations: “*Internet and the Law – Disturbances and Early Sorrow*”. *In*: CHATILLON, Georges (Ed.) - ***Internet International Law: International and European Studies and Comments***. Bruxelas: Bruylant, 2005, pp. 211-219. P. 217.

¹⁸⁷ BUTTARELLI, Giovanni - *The General Data Protection Regulation: Making the world a better place?*, 2015, p. 4.

De certa forma, a proteção de dados impõe a adoção de regras que combatam as práticas de monopólio. O seu cumprimento gera vantagens económicas e de reputação, através de soluções técnicas e tecnológicas que protejam os dados e que confirmem confiança aos utilizadores dos serviços oferecidos por essas empresas. Aliás, o Regulamento concede responsabilidade para entender o espírito e a letra da lei às empresas, mas com fortes sanções para o incumprimento das regras destinadas a proteger os indivíduos. Além disso, as noções de equidade, transparência e respeito pelos indivíduos devem ser integradas na tomada de decisões.

5.2. Atual Regime de Proteção de Dados na UE

A relação entre a proteção de dados pessoais e os Direitos Fundamentais, nos Estados-Membros, pode ser classificada de diversos modos:

- ✚ O direito à proteção de dados é concebido para servir, primariamente, outros direitos, como o direito à privacidade, como é o caso da Bélgica;
- ✚ A proteção de dados está conectada a um direito fundamental *sui generis*, reconhecido na Constituição ou em norma com valor constitucional, como acontece na Hungria e pode considerar-se que Portugal está incluído nesta categoria;
- ✚ Existe, na Constituição, um mandato para legislar na proteção de dados pessoais, de que é exemplo a Finlândia;
- ✚ O TC estabeleceu um direito *sui generis*, apesar de a Constituição não o acolher abertamente, tal como na Alemanha; e
- ✚ Trata-se a relação da proteção de dados pessoais e de direitos fundamentais de modo incerto, como se verifica na Dinamarca.

Muitas vezes, porém, torna-se difícil atribuir um modelo. Além disso, quando a Carta foi elaborada, poucos Estados-Membros tinham uma abordagem de reconhecimento explícito do direito à proteção de dados.¹⁸⁸

¹⁸⁸ FUSTER, Gloria – *Op. cit.*, 2014, pp. 174-175.

Seguindo o entendimento de Orla Lynskey, o regime de proteção de dados da UE caracteriza-se por quatro traços essenciais: regime global (*omnibus regime*), legitimante, baseado em direitos e com impacto extraterritorial.¹⁸⁹

Quanto à sua natureza de “*omnibus regime*”, esta diz respeito à distinção quanto aos regimes que governam o tratamento de dados, que podem ser, de forma ampla, categorizados como *omnibus* ou globais (como o da UE) ou setoriais (ou limitados). No primeiro caso, o qual importa na presente situação, as regras de proteção de dados aplicam-se tanto a atores públicos como a privados, apesar de existirem *de facto* regras distintas para o tratamento no que toca à área da política externa comum e de segurança e ao campo da cooperação policial e judicial.

A segunda particularidade deste regime diz respeito ao facto de ser **legitimante**, isto é, uma vez demonstrado que a base legal para o tratamento existe e que tal tratamento cumpre as garantias específicas de proteção de dados relacionadas com qualidade de dados definidas em legislação secundária, então este tratamento é, em princípio, legítimo.

O regime de proteção de dados da UE é, ainda, considerado um **regime baseado em direitos**. Esta orientação foi reforçada com a Carta, em 2000, e com o Tratado de Lisboa, em 2009. Tal característica pode ser aferida tendo em conta dois ângulos de ideias:

- ✚ Garante direitos aos indivíduos;
- ✚ Confere expressão a um direito fundamental diretamente ou o seu *design* e interpretação são consistentes com a sua conceção subjacente como direito fundamental.

Por um lado, a Diretiva garante vários direitos subjetivos aos indivíduos e esses direitos foram reiterados no Regulamento. Aliás, o Regulamento adiciona condições e garantias para os direitos garantidos pela Diretiva. Por outro lado, defende-se que o enquadramento regulatório para a proteção de dados da UE é consistente com a conceção subjacente da privacidade informacional como direito humano

¹⁸⁹ LYNKEY, Orla, *Op. cit.*, 2015, pp. 15-41.

fundamental. Este caráter de direito fundamental reflete-se no *design* e interpretação das regras europeias. Aliás, o TJ, explicitamente, confirmou que a Diretiva deve ser interpretada à luz dos Direitos Fundamentais, como supramencionado, no 3.º Capítulo, com as referências aos Acórdãos *Rundfunk* e *Promusicae*.

Apesar das vigorosas políticas de unificação e de prevenção de disparidades entre os sistemas legais da UE, dificilmente é atingido o consenso e, assim, a UE, em nome da sua soberania, realça a escolha dos valores refletidos na sua legislação.¹⁹⁰

O alto nível de proteção padrão oferecido pelo regime da UE à proteção de dados é outro potencial indicador do seu caráter de direito fundamental. Ao regular, o legislador da UE optou por evitar abordagens de direito privado em matéria de proteção de dados pessoais, como, por exemplo, conceder aos particulares direitos de propriedade sobre os seus dados pessoais ou permitir que os indivíduos celebrem acordos de contacto que reflitam melhor as suas próprias preferências de proteção de dados. Uma explicação para a rejeição destas soluções de direito privado, apesar dos seus potenciais benefícios, é que a UE procura decretar um regime de proteção de dados que não seja contornado através de acordos privados, devido ao seu caráter de direito fundamental.¹⁹¹

O “*Article 29 Data Protection Working Party*” defende que o enquadramento de proteção de dados da UE oferece um “mínimo e não negociável nível de proteção da privacidade para todos os indivíduos.”. Assim sendo, uma pessoa não pode escolher contratar privadamente afastando os seus direitos.

A quarta característica do regime europeu é referente ao seu **caráter extraterritorial**. Assim, a proteção de dados constitui um dos campos em que a UE exerce supremacia regulatória global, uma vez que o seu regime influencia o resto do mundo.

É sugerido que, enquanto no passado, sob a Diretiva, esta supremacia ocorreu por defeito, o Regulamento pode levar a uma supremacia por conceção. A supremacia

¹⁹⁰ POULLET, Yves – *Op. cit.*, 2005, p. 164.

¹⁹¹ LYNSKEY, Orla, *Op. cit.*, 2015, p. 40.

por defeito originou-se devido à proibição da transferência de dados da UE para países terceiros que não ofereçam um nível adequado de proteção, como definido no art. 25.º da Diretiva, o que requeria que estes tivessem regras similares às europeias. A avaliação pela Comissão Europeia, que tem sido muito lenta, conduziu ao denominado “efeito de Bruxelas” das regras de proteção de dados da UE. Já relativamente à supremacia por conceção, originada pelo Regulamento, esta tem lugar uma vez que se permite à Comissão reconhecer a adequação de um maior volume de entidades. Além disto, o âmbito territorial do Regulamento é estendido ao tratamento de dados de titulares residentes na União, efetuado por responsável estabelecido num terceiro país, quando as atividades de tratamento cumpram certos requisitos, o que demonstra esta supremacia por conceção.¹⁹²

Quanto ao propósito das regras de proteção de dados, existem duas perspetivas: ora são encaradas como uma regulação orientada para os direitos ou como uma regulação económica. Ou seja, ou servem para assegurar a privacidade da informação dos cidadãos individuais ou servem para permitir às empresas privadas e autoridades públicas utilizar o valor integrado nos dados pessoais, contribuindo para a economia digital. Aplicada à *Internet*, a questão torna-se saber se as regras de proteção de dados servem para a tornar um ambiente seguro para os seus utilizadores ou se têm como objetivo transformá-la num *forum* produtivo de tratamento de dados pessoais. As regras de proteção de dados podem ser consideradas uma espécie híbrida com elementos de ambas as regulações.¹⁹³

A AEPD refere que só é possível usufruir dos potenciais benefícios das TIC se estas suscitarem confiança nos seus utilizadores. Por sua vez, essa confiança apenas será conquistada se estas tecnologias forem fiáveis e seguras, se as pessoas sentirem que elas estão sob o seu controlo e que a proteção da sua privacidade e dos seus dados pessoais está garantida. Da mesma forma, a privacidade e a proteção de dados

¹⁹² *Ibidem*, pp. 41-43.

¹⁹³ BLUME, Peter – *Op. cit.*, 2015, p. 6.

devem estar inseridas em todo o ciclo de vida da tecnologia, optando-se por uma abordagem de “privacidade desde a conceção”.¹⁹⁴

Assim, as soluções sugeridas por esta Autoridade passam por um investimento na educação dos utilizadores da *Internet*, um melhor aproveitamento do papel da auto-regulação, como é o caso do acordo estabelecido entre a Comissão e diversos fornecedores de redes sociais denominado “Princípios para redes sociais mais seguras na UE” e uma necessidade de fornecimento de definições de “privacidade por defeito” obrigatórias aos utilizadores de serviços *online* para que possam controlar as suas informações pessoais.

5.3. Direito Fundamental à proteção de dados pessoais no Regulamento Geral

O art. 16.º do TFUE garante o direito à proteção de dados pessoais com efeito direto, manifestando-se nas áreas policial e de cooperação judicial. O seu âmbito de aplicação abrange as instituições, órgãos, organismos da UE e os Estados-Membros. A exceção do n.º 2, que estabelece que “*O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de actividades relativas à aplicação do direito da União, e à livre circulação desses dados*”, faz prevalecer o art. 39.º do TUE quando se esteja perante normas específicas de política externa e de segurança comum e, nesses casos, é o Conselho que adota uma decisão relativa a esta matéria.

De acordo com o art. 8.º da Carta, o direito à proteção de dados envolve condições de legitimidade para o tratamento, direitos que se assumem como corolários necessários e condições garantística, os quais serão analisados de seguida.

¹⁹⁴ HUNSTINX, Peter - Parecer da AEPD sobre a promoção da confiança na sociedade da informação através do reforço da protecção dos dados e da privacidade (2010/C280/01), de 16 de outubro de 2010, pontos 16 e 19.

A autodeterminação informacional reveste a natureza de posição jurídica complexa, abrangendo ela própria diferentes posições jurídicas ativas (direitos, liberdades, garantias e poderes) que compõem os direitos fundamentais.

Desta forma, a proteção de dados assume-se como um direito complexo composto por elementos próprios de direitos, liberdades e garantias.¹⁹⁵

5.2.1. Princípios orientadores da proteção de dados

Quando se preenchem as condições que legitimam o tratamento de dados pessoais, devem respeitar-se diversos princípios orientadores destas operações, os quais se passam a especificar.

O Capítulo II do Regulamento é relativo aos “**Princípios**”. Estes princípios orientadores do tratamento de dados pessoais encontram-se elencados no art. 5.º.

A al. a) do n.º 1 do art. 5.º é referente aos **princípios da licitude, da lealdade e da transparência**, que impõem que os dados pessoais sejam objeto de um tratamento lícito, leal e transparente.

De modo a averiguar do conteúdo da base de dados, e se a sua criação respeita as exigências de necessidade e adequação social, deve existir clareza e transparência dos registos quanto às categorias de dados recolhidos, existência de fluxos de informação, tempo de tratamento e identificação dos responsáveis.¹⁹⁶

Por sua vez, a al. b) do mesmo artigo, refere-se ao **princípio da limitação das finalidades**, que estabelece que os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

Este princípio parece ser incompatível com o atual mundo do *Big Data*, no qual os dados são, regularmente, utilizados de novas e diferentes formas.

¹⁹⁵ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 827.

¹⁹⁶ MONIZ, Helena – *Op. cit.*, 1997, p. 263.

A al. c) respeita ao **princípio da minimização dos dados**, o qual determina que os dados devem ser adequados, pertinentes e limitados ao necessário em relação às finalidades do tratamento.

Apenas é lícita a recolha e tratamento de dados relacionados diretamente com as finalidades do tratamento, isto é, os dados devem ser restringidos ao necessário para cumprirem as finalidades para as quais são tratados.

De acordo com este princípio, os dados pessoais podem ser objeto de tratamento apenas se forem adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com a recolha e/ou o tratamento. A aplicação deste princípio implica a necessidade de avaliar se os meios utilizados para o tratamento dos dados e os tipos de dados pessoais utilizados são adequados e têm possibilidades razoáveis de atingir os seus objetivos.¹⁹⁷

Já a al. d) institui o **princípio da exatidão**, exigindo que os dados sejam exatos e atualizados relativamente às finalidades do seu tratamento, devendo ser apagados ou retificados sem demora caso sejam inexatos.

Seguidamente, a al. e) consagra o **princípio da limitação da conservação**, conforme o qual os dados pessoais apenas podem ser conservados, de forma a permitir a identificação dos titulares, durante o período necessário para as finalidades do tratamento.

Ou seja, uma vez satisfeita a finalidade do tratamento desses dados, devem os mesmos ser retirados das bases de dados em que se encontram a ser tratados.

Relativamente à al. f), é estabelecido o **princípio da integridade e confidencialidade**, que refere que os dados pessoais apenas podem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental.

¹⁹⁷ Ponto 69 do Parecer da Autoridade Europeia para a Proteção de Dados sobre a neutralidade da *Internet*, a gestão do tráfego e a proteção da privacidade e dos dados pessoais (2012/C 34/01), de 8 de fevereiro de 2012.

Estes princípios efetivam-se em medidas necessárias a evitar a perda, destruição, alteração, falsificação, sabotagem e acesso não autorizado a ficheiros de dados pessoais.

Para além disto, os titulares têm, ainda, no âmbito do art. 33.º do Regulamento, o direito de saber se os seus dados pessoais foram alvo de pirataria informática, ou seja, as empresas e as organizações devem informar, prontamente, as pessoas sobre as violações graves em matéria de proteção de dados. Devem, além disso, notificar a competente autoridade de controlo da proteção de dados.

Por fim, no n.º 2 do art. 5.º, estabelece-se o **princípio da responsabilidade**, segundo o qual o responsável pelo tratamento é responsável pelo cumprimento de todos os princípios acima referidos e tem de poder comprová-lo.

Devem ser cumpridos os requisitos de legitimidade do tratamento e respeitados e efetivados os direitos do cidadão. Logo, é necessária a imposição legal de deveres especiais e regras deontológicas para os responsáveis pelos ficheiros.¹⁹⁸

Os artigos seguintes deste Cap. II dizem respeito às condições que asseguram a licitude do tratamento, consoante o tipo de dado pessoal em causa.

De acordo com Catarina Sarmento e Castro, existem três princípios gerais, a saber: o **princípio geral da transparência**, de acordo com o qual o responsável do tratamento deve dar a conhecer ao titular a realização do tratamento que lhe respeite, princípio este que se efetiva através dos direitos à informação e de acesso, e tem expressão no dever de notificação dos tratamentos, o **princípio da finalidade**, que estabelece que os dados só podem ser utilizados para a finalidade determinante da recolha e que inclui o princípio da limitação do uso dos dados, e, por fim, os **princípios relativos à qualidade dos dados**, que se concretizam através dos princípios da licitude e

¹⁹⁸ MONIZ, Helena – *Op. cit.*, 1997, p. 265.

lealdade, princípios da adequação, pertinência e proporcionalidade e princípios da exatidão e atualização dos dados.¹⁹⁹

Existem autores que acrescentam um princípio da justificação social, o qual se prende com a obrigatoriedade de apenas se criar ficheiros de dados pessoais necessários para a organização da sociedade, isto é, apenas se deve proceder à criação e manutenção de ficheiros com objetivos ou finalidades que correspondam a interesses socialmente adequados, e um princípio da publicidade, segundo o qual a criação da base deve ser publicitada, deve haver conhecimento da sua criação e manutenção, com fins de controlo das bases e potenciais ameaças a direitos fundamentais.²⁰⁰

5.2.2. Conteúdo do direito à proteção de dados

Ao titular dos dados é conferido um conjunto de direitos para salvaguardar o seu direito à autodeterminação informativa. É um verdadeiro feixe de prerrogativas que asseguram que cada um decida sobre onde, como e a quem são transmitidos os seus dados. É um poder de dispor e de controlar os dados pessoais.

Aos direitos conferidos aos titulares dos dados pessoais correspondem, da mesma forma, deveres para os responsáveis pelo tratamento desses dados. Assim sendo, e enquanto direito complexo, o direito à proteção de dados engloba tanto direitos como deveres e garantias.

5.2.2.1. Direitos dos titulares de dados pessoais

Sendo o controlo dos dados pessoais um aspeto do direito à proteção de dados, resta a dúvida sobre se constituirá a sua essência ou a periferia. Se for de essência, apenas excecionalmente pode sofrer limitações, enquanto se for de periferia, de acordo com o n.º 1 do art. 52.º da CDFUE, pode ser limitado para objetivos de

¹⁹⁹ CASTRO, Catarina Sarmento – *Op. cit.*, 2005, pp. 229-237.

²⁰⁰ MONIZ, Helena – *Op. cit.*, 1997, p. 262.

interesse geral ou para proteger direitos e liberdades de outros.²⁰¹

Pode considerar-se o controlo dos dados pessoais como âncora normativa no regime da proteção de dados da UE. Aliás, no acórdão *Google Spain*, o Tribunal implicitamente considerou o controlo dos indivíduos sobre os dados pessoais como uma faceta do direito à proteção de dados.

Apesar do consenso sobre a sua importância, o princípio do controlo individual raramente está contido numa regra singular a si referente.

O reconhecimento do controlo como elemento constitutivo do regime da proteção de dados tem impacto na noção de consentimento pois reafirma a preferência da UE no consentimento *opt-in*, isto é, na expressão da vontade do titular dos dados em permitir o tratamento.²⁰²

O consentimento constitui uma das bases legais sobre as quais o responsável dos dados pode legitimamente tratar os dados pessoais, e este consiste numa manifestação de vontade que implica uma exteriorização que possa ser comprovada, a qual deve ser livre (manifestada sem intervenção de qualquer coação), específica (concreta e precisa) e informada (o titular deve estar ao corrente dos efeitos do seu consentimento).²⁰³

O tratamento contra ou sem o consentimento do titular dos dados é uma violação gravíssima dos direitos de personalidade. Só deve ter lugar quando se torne absolutamente indispensável e imprescindível por exigências de um interesse público claramente superior. Quanto estejam em causa direitos de personalidade, será necessário encontrar um fundamento de ordem pública, uma necessidade insuperável de interesse coletivo, que não permita uma solução alternativa e que justifique eticamente tal agressão. Quando assim for, a agressão deverá ser o mais limitada possível, para reduzir ao mínimo a lesão do direito à privacidade.²⁰⁴

²⁰¹ LYNKEY, Orla, *Op. cit.*, 2015, p. 175.

²⁰² *Ibidem*, pp. 185-186.

²⁰³ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, pp. 261-262.

²⁰⁴ VASCONCELOS, Pedro Pais de – *Op. cit.*, 1999, pp. 251-253.

De acordo com a al. 11) do art. 4.º do Regulamento, “consentimento” consiste numa “*manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*”. Quando este consentimento se verificar, o tratamento dos dados pessoais da pessoa que consentiu, torna-se lícito, conforme estabelece a al. a) do n.º 1 do art. 6.º. Porém, poderá haver tratamento de dados sem o consentimento do titular por razões de interesse público, tal como referido nos Considerandos n.º 54 e seguintes do Regulamento.

Quando o tratamento se encontra legitimado, devem, então, respeitar-se os direitos dos titulares dos dados.

O Cap. III do Regulamento Geral consagra os “**Direitos do titular dos dados**”. Este Capítulo encontra-se dividido em cinco Secções:

Secção 1 – Transparência e regras para o exercício dos direitos dos titulares dos dados: Art. 12.º

Secção 2 – Informação e acesso aos dados pessoais: Arts. 13.º a 15.º

Secção 3 – Retificação e apagamento: Arts. 16.º a 20.º

Secção 4 – Direito de oposição e decisões individuais automatizadas: Arts. 21.º a 22.º

Secção 5 – Limitações: Art. 23.º

Deste modo, assinalam-se, separadamente, os direitos estabelecidos neste Regulamento.

A) Na Secção 1, o art. 12.º diz respeito ao direito à “Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados”, e impõe ao responsável pelo tratamento dos dados a tomada de medidas que forneçam ao titular as informações de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Pode considerar-se como um **direito ao conhecimento**, isto é, o direito do titular a

conhecer o conteúdo da base de dados e os dados a si respeitantes existentes nos registos informáticos.

B) Já na Secção 2, os arts. 13.º e 14.º, os quais estão divididos consoante os dados sejam recolhidos direta ou indiretamente, concernem ao **direito de informação**, no sentido em que o responsável pelo tratamento dos dados deve facultar diversas informações ao titular dos dados aquando da sua recolha, concretamente a identidade e contactos dos responsáveis, os contactos do encarregado da proteção de dados, as finalidades do tratamento, os interesses legítimos do responsável em certas situações, os destinatários dos dados e, se for caso disso, a intenção de transferir os dados para um país terceiro ou organização internacional. Além destas informações, o n.º 2 do art. 13.º e o n.º 2 do art. 14.º determinam outro conjunto de informações que devem ser fornecidas ao titular, a fim de garantir um tratamento equitativo e transparente, como é o caso do prazo de conservação dos dados pessoais.

Este direito assegura o tratamento leal e transparente, manifestando-se, até, como elemento próprio e necessário da autodeterminação informacional.²⁰⁵

Assim, o tratamento não decorre de forma lícita quando o titular dos dados desconheça que este se realiza ou não conheça alguns dos aspetos fundamentais desse tratamento.²⁰⁶

Enquanto a Diretiva não previa a situação de o responsável pelo tratamento inicial pretender utilizar os dados para outros fins, o Regulamento faz menção a esta hipótese, determinando, no n.º 3 do art. 13.º e no n.º 4 do art. 14.º, que a informação fornecida ao titular dos dados deve ser renovada, relativamente às novas finalidades e quaisquer outras questões relevantes.

C) No art. 15.º encontra-se regulado o **direito de acesso**, que se consubstancia no corolário do regime de proteção de dados da UE. Deste modo, tem o titular o

²⁰⁵ PINHEIRO, Alexandre Sousa – *Op. cit.*, 2015, p. 659.

²⁰⁶ CASTRO, Catarina Sarmento – *Op. cit.*, 2005, pp. 242-243.

direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se forem, o direito de aceder a esses dados e a um conjunto de informações que se encontram enumeradas no artigo em causa.

Este direito deriva do princípio de que os dados devem ser comunicados de forma inteligível, pela Diretiva, ou, quando tratados eletronicamente, de forma eletrónica e interoperável, de acordo com o Regulamento.²⁰⁷

O direito de informação distingue-se do direito de acesso, uma vez que aquele antecede e determina as condições de recolha, enquanto este permite acompanhar as vicissitudes dos tratamentos. Este direito caracteriza-se pelo facto de não depender de invocação da finalidade e não poder ser limitado por motivos de legitimidade ou qualquer outra justificação do responsável pelo tratamento.

Na Diretiva, era conferida uma ampla margem de conformação aos Estados na forma de concretizar este direito, porém, com a adoção do Regulamento, este direito torna-se uniforme no território de todos os Estados-Membros.

Enquanto corolário do direito à autodeterminação informativa, apenas deverão existir limites de harmonia com os princípios da necessidade, proporcionalidade e adequação.²⁰⁸

Este direito conduz, por sua vez, a mecanismos de correção dos dados, como o direito à retificação dos dados pessoais inexatos, incompletos ou equívocos, assim como à sua atualização.

D) Relativamente à Secção 3, o art. 16.º começa por estabelecer o **direito de retificação**, que determina que o titular pode obter, sem demora injustificada, da parte do responsável pelo tratamento, a retificação dos seus dados inexatos e o completamento dos dados incompletos. Assim, tem o responsável pelo tratamento o dever de retificar, em prazo razoável e sem custos excessivos para o titular.

²⁰⁷ LYNKEY, Orla, *Op. cit.*, 2015, p. 180.

²⁰⁸ MONIZ, Helena – *Op. cit.*, 1997, pp. 252-253.

Pode considerar-se que também engloba um direito à atualização de dados desatualizados, como forma de respeitar o princípio da exatidão e atualização, uma vez que o próprio princípio da qualidade dos dados obriga à garantia deste direito.²⁰⁹

E) O direito consagrado no art. 17.º reveste-se de particular sensibilidade, dado o debate que teve lugar em torno do mesmo e que acabou por conduzir à consagração deste **direito ao apagamento dos dados** (“direito a ser esquecido”).

No n.º 1 deste artigo, confere-se ao titular o direito de obter o apagamento dos seus dados pessoais, sem demora injustificada, quando os dados deixem de ser necessários para a finalidade prosseguida com a sua recolha ou tratamento, quanto o titular retire o seu consentimento para o tratamento e não haja outro fundamento legitimador do mesmo, quando o titular se oponha ao tratamento, quando os dados forem tratados ilicitamente, quando os dados tenham de ser apagados de forma a cumprir uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável esteja sujeito e quando os dados tiverem sido recolhidos no contexto de uma oferta de serviços.

O n.º 2 do mesmo artigo estabelece que, quando este responsável tenha tornado os dados públicos, e for obrigado a apagá-los, deve tomar as medidas que forem razoáveis para informar os responsáveis efetivos de que o titular solicitou o apagamento das ligações para esses dados, e as suas cópias e as reproduções.

Com este segundo número do artigo, observa-se que o Regulamento juntou o direito a ser esquecido ao direito a apagamento.²¹⁰

Existe, porém, muita confusão terminológica e concetual quanto a estes termos. Assim, devemos distinguir entre o “*right to oblivion*”, que consiste no direito de ser livre de um passado judicial ou criminal, o “*right to erasure*”, ou seja, o direito de apagamento, o direito a remover ou apagar dados através de legislação de proteção de dados, pelo facto de os dados só poderem ser tratados e armazenados pelo período necessário, e o “*right to be forgotten*”, isto é, o direito a ser esquecido, a ter os

²⁰⁹ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, p. 250.

²¹⁰ FUSTER, Gloria – *Op. cit.*, 2014, p. 245.

seus dados pessoais *online* removidos ou ter o acesso aos mesmos restringido, sobretudo em contexto de aplicações geradas pelo utilizador. Este último compreende direitos relacionados com a remoção de dados dos índices dos motores de busca e dos arquivos digitais.²¹¹

O direito a ser esquecido, ou direito ao esquecimento, diretamente motivado pela *Internet*, apesar de ser um conceito atrativo, é difícil de alcançar. Vai mais além do dever de o responsável pelo tratamento apagar dados incorretos. Baseia-se na premissa de que, enquanto, antes, o decurso do tempo levava ao esquecimento, com o advento das novas tecnologias, a memória perdura e a *Internet* não esquece nem perdoa. Desta forma, mesmo quando o responsável pelo tratamento os apaga, estes podem já ter sido capturados através dos mecanismos de busca e estar localizados fora do alcance do responsável.

Devido ao armazenamento *online* de grandes quantidades de dados pessoais, que persistem no tempo, da sua pronta acessibilidade e da partilha intensiva de dados, coloca-se o problema da “eternidade digital”. Só a definição de um tempo de conservação dos dados pode impedir a apropriação perpétua de amplas facetas da vida pessoal. Porém, devido a obstáculos técnicos, a *Internet* torna impossível fazer cumprir total e efetivamente tal direito, uma vez que apagar as hiperligações não implica que os dados desapareçam, apenas as torna mais difíceis de encontrar. Porventura, seria mais certo denominar-se “direito a ser mais dificilmente recordado”.²¹²

O direito a ser esquecido, estabelecido no Regulamento consiste numa tentativa de lidar com os problemas da eternidade digital, estendendo o conceito do direito ao “*erasure*” para que se aplique aos dados online persistentes.²¹³

Por vezes, sugere-se que este problema seja resolvido por meios extralegais, através de soluções baseadas em tecnologia, tal como é o caso da sugestão de que

²¹¹ LINDSAY, David – *Op. cit.*, 2014, p. 292.

²¹² BLUME, Peter – *Op. cit.*, 2015, pp. 10-11.

²¹³ LINDSAY, David – *Op. cit.*, 2014, p. 313.

aplicações, como a do *Snapchat app*, contenham um mecanismo de apagamento automático.

Contudo, o direito ao esquecimento não pode ser assegurado através de abordagens técnicas, dado que os dados pessoais são inerentemente vulneráveis a cópias e reproduções não autorizadas.²¹⁴

Há limites inerentes às soluções legais para os problemas da eternidade digital. Por exemplo, as pessoas não devem ser dissuadidas de se conter na publicação das suas informações pessoais, com a falsa expectativa de que têm o direito legal ao seu subsequente apagamento.

Na Diretiva, o apagamento de dados ficava aquém do “*right to erasure*” e não incorporava qualquer direito ao esquecimento.²¹⁵

Assistimos, assim, à interseção de dois esforços complexos: a tentativa de proteger o direito à privacidade e o direito à proteção de dados pessoais, no contexto de dados pessoais persistentes e acessíveis *online* e as propostas para a reforma fundamental europeia em matéria de proteção de dados. Mas este direito não foi concebido para dar a solução perfeita aos problemas da eternidade digital, tão-somente, para reforçar o direito dos titulares dos dados a terem os seus dados removidos quando tal é possível e legítimo.²¹⁶

Por último, assinala-se que, se um utilizador individual copiar um ficheiro de outrem como, por exemplo, uma fotografia, e o partilhar na *Internet*, o Regulamento pode não se aplicar devido à “*household exemption*”, ou seja, a exceção das atividades puramente domésticas, às quais não se aplica o Regulamento, e, então, o lesado terá de ativar outros mecanismos legais, como ações civis por desrespeito à privacidade.

Há decisões políticas que devem ser tomadas, no contexto deste direito, que dizem respeito, nomeadamente, à questão de saber se os utilizadores individuais devem ser

²¹⁴ Relatório da Agência da União Europeia para a Segurança das Redes e da Informação “*The right to be forgotten – between expectations and practice*”. Heracião: ENISA. P. 14.

²¹⁵ LINDSAY, David – *Op. cit.*, 2014, p. 309.

²¹⁶ *Ibidem*, pp. 331-333.

tratados como responsáveis de dados e ao facto de qualquer obrigação de remover material, especialmente do *SNS* ou da *Internet*, pode, na prática, infringir o direito à liberdade de expressão de partes terceiras.²¹⁷

F) O art. 18.º consagra o **direito à limitação do tratamento**, o qual será garantido caso se verifique alguma das situações referidas nas suas alíneas. Caso se concretize, os dados pessoais só poderão, à exceção da conservação, ser tratados com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro, tal como definido no n.º 2 do citado artigo.

A obrigação de notificação de retificação ou apagamento dos dados pessoais ou limitação do tratamento encontra-se delimitada no art. 19.º.

G) O último artigo da Secção 3, o art. 20.º, reconhece o novíssimo **direito de portabilidade dos dados**, o qual permite aos titulares dos dados obter uma cópia dos seus dados pessoais, os quais foram fornecidos ao responsável pelo tratamento, para que os possa transmitir a outro responsável de tratamento, nas condições previstas no referido artigo. Este direito permite, para os titulares de dados, reduzir os custos da mudança de um provedor de serviços eletrónicos para outro. Há quem considere que este direito constitui, mais, um direito do consumidor, do que um verdadeiro direito fundamental inserido no direito à proteção de dados.

H) Por sua vez, a Secção 4 inicia-se com a definição do **direito de oposição**, no art. 21.º. De acordo com este direito, o titular dos dados pode opor-se, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais referidos nesse artigo. Assim, “*O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse*

²¹⁷ *Ibidem*, pp. 336-337.

tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.”.

Este direito constituiu uma inovação em matéria de direitos fundamentais, e deve ser interpretado como forma de atenuar as limitações dos direitos dos indivíduos que resultam da aceitação do consentimento implícito em algumas circunstâncias. Deve ser encarado como uma garantia adicional e não como um direito subsidiário do direito de acesso.

Este direito apresenta-se como uma consequência do direito de controlo de cada cidadão sobre o uso dos seus dados pessoais, podendo este recusar-se a responder a algo, mas também opor-se a que os dados cujo fornecimento não dependa de si sejam tratados. Deste modo, o direito de oposição assume a sua verdadeira dimensão quando o tratamento é leal e lícito, pois, mesmo assim, o titular pode apresentar razões que justifiquem a sua recusa.

I) Finalmente, o art. 22.º determina o **direito de não ficar sujeito a decisões individuais automatizadas**, no sentido de que o titular dos dados tem o direito de não ficar adstrito a uma decisão, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, tomada exclusivamente com base num tratamento automatizado, o que inclui a definição de perfis. Não se permite que decisões relevantes sobre a vida de uma pessoa se fundamentem apenas num tratamento de dados pessoais, consagrando-se, desta forma, uma proibição geral.

A Secção 5 contém apenas o art. 23.º relativo a possíveis restrições, efetuadas pelo Direito da UE ou dos Estados-Membros, relativas a princípios específicos e aos direitos consagrados nos arts. 12.º a 22.º, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir certos princípios ou valores, os quais se encontram elencados no art. 23.º. O Considerando 73.º do Regulamento refere, a este propósito, que “*Essas restrições deverão respeitar as exigências*

estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.”.

Depois da análise dos direitos incluídos no direito ao controlo dos dados pessoais à luz do atual Regulamento, assinala-se um mais antigo entendimento da maioria da doutrina relativamente às três grandes vertentes do direito à autodeterminação informacional e o qual ainda se apresenta correto, apesar de necessárias adaptações. Assim, o direito ao controlo dos dados pessoais informatizados (que engloba o direito de acesso, o direito de conhecimento, o direito ao esclarecimento, o direito de retificação ou contestação dos dados, o direito de atualização e o direito de eliminação de informações incorretas), o direito à não difusão de dados pessoais informatizados (o qual inclui uma proibição geral de acesso de terceiros e de fluxo transfronteiriço de dados) e o direito ao não tratamento informatizado de dados sensíveis.²¹⁸

De acordo com outra estrutura doutrinária, o direito de controlo abrangeria quatro poderes relativamente aos dados pessoais informatizados: o poder de conhecer o seu teor, de conhecer a sua finalidade, de exigir a sua retificação (o que pode incluir operações de substituição, supressão e completamento), e o poder de exigir a sua atualização (o qual abarca as mesmas operações). O direito à não difusão dos dados pessoais englobaria uma vertente subjetiva de evitar o conhecimento dos dados por terceiros e uma vertente objetiva de impedir a interconexão de ficheiros. Do conceito de terceiro deve ser excluído o conjunto de pessoas cuja profissão se relaciona com as diversas operações inerentes ao processamento automatizado desses, bem como os responsáveis pelos ficheiros. Por fim, o direito à proibição do tratamento informatizado dos dados pessoalíssimos (ou sensíveis, como na divisão anteriormente referida) relaciona-se, de perto, com a intimidade da pessoa.²¹⁹

²¹⁸ MONIZ, Helena – *Op. cit.*, 1997, pp. 252-261.

²¹⁹ GOUVEIA, Jorge Bacelar – *Op. cit.*, 1991, pp. 718-729.

Com o novo Regulamento Geral, o art. 9.º refere como proibido o “tratamento de categorias especiais de dados pessoais”, as quais revelam “*a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*”.

Assim, mantém-se o referido “direito ao não tratamento de dados sensíveis”. Esta proibição poderá ser ultrapassada através do preenchimento de qualquer uma das condições estabelecidas no n.º 2 do art. 9.º, e entre as quais figura o caso do consentimento explícito do titular dos dados.

5.2.2.2. Deveres dos responsáveis de tratamento de dados pessoais

Os deveres dos responsáveis pelo tratamento de dados traduzem-se no correspondente direito do titular dos dados, ou resultam da consagração legal dos princípios gerais de proteção.²²⁰

Os deveres que correspondem a direitos dos titulares dos dados são:

- ✚ Dever de legalizar os tratamentos;
- ✚ Prestar informações ao titular;
- ✚ Garantir o exercício do direito de acesso, correção e eliminação dos dados pessoais pelo titular;
- ✚ Assegurar o exercício do direito de oposição;
- ✚ Retificar os dados pessoais inexatos sem demora injustificada;
- ✚ Apagar os dados pessoais que o titular requeira, e, quando os tenha tornado públicos, tomar as medidas necessárias para informar os restantes responsáveis pelo tratamento de que o titular solicitou o apagamento das ligações, das cópias e das reproduções; e
- ✚ Limitar o tratamento em certas condições e transmitir cópia dos dados pessoais ao titular para que este os possa transferir para outro provedor de serviços.

²²⁰ CASTRO, Catarina Sarmiento – *Op. cit.*, 2005, pp. 263-265.

Os deveres que advêm dos princípios gerais são:

- ✚ Impossibilidade de recolher dados em violação do princípio da lealdade, da transparência e da licitude;
- ✚ Não tratar os dados para finalidades que não as iniciais;
- ✚ Tratar os dados que são adequados, pertinentes e limitados aos objetivos do tratamento;
- ✚ Não tratar dados sensíveis (salvo nos casos previstos na lei);
- ✚ Não conservar os dados além da duração estabelecida;
- ✚ Garantir a segurança do tratamento, no sentido da sua integridade e confidencialidade (existindo a obrigação de sigilo profissional); e
- ✚ Dever de responsabilidade pelo cumprimento dos princípios assinalados.

Vale a pena assinalar que a função das autoridades de controlo do tratamento de dados pessoais é mais reativa do que preventiva na tutela do direito à proteção de dados.²²¹

Com a globalização dos mercados, cria-se a necessidade de normas reguladoras dos fluxos de dados dos Estados-Membros com destino a países terceiros, o que é essencial para que os responsáveis pelo tratamento saibam as regras de proteção de dados a que estão sujeitos e que dados podem ser transferidos.

A este propósito, assinala-se que, ao nível do Direito da UE, em vez do critério de equivalência utilizado na Convenção n.º 108, é utilizado um critério de adequação para que se permita a transferência de dados para países terceiros, sendo necessário aferir se o nível de proteção conferido por esse Estado terceiro é adequado, através de uma análise quanto à obediência aos princípios fundamentais de proteção de dados consagrados nas legislações destes países.

²²¹ CALVÃO, Filipa – *Op. Cit.*, 2015, p. 47.

Relativamente a esta transferência para países terceiros, o dispositivo comunitário procura conciliar os interesses de salvaguarda de informação pessoal, com a necessidade de tratamento e circulação dos dados pessoais por parte de terceiros.

Quanto à transferência para países da UE, respeita-se o princípio da liberdade de circulação dos dados pessoais, que é consequência do estabelecimento de regras comuns de proteção, resultado do nível de proteção equivalente resultante da aproximação das legislações nacionais, conforme se verifica no n.º 3 do art. 1.º do Regulamento.

O Regulamento conta com diversas inovações, das quais merece referência, nomeadamente, a existência de obrigatoriedade de encontrar soluções tecnológicas que sejam, ou adotadas de raiz com o sistema no qual se procede ao tratamento de dados (a *privacy by design*), ou utilizadas como solução supletiva, por defeito (a *privacy by default*).²²² Estas regras relevam por evidenciarem a referida necessidade de combinação dos instrumentos com as novas tecnologias de modo a, mais eficazmente, se protegerem os Direitos Fundamentais.

Em suma, como referido pela atual AEPD, *“cabe agora às empresas e outras organizações, que investem muito esforço na descoberta de modos inovadores para utilizar dados pessoais, utilizar o mesmo espírito inovador sempre que implementarem legislação em matéria de proteção de dados.”*²²³

²²² CALVÃO, Filipa – O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento. *In: Fórum de Proteção de Dados*, n.º 1, 2015, pp. 37-48. P. 44.

²²³ BUTTARELLI, Giovanni - Parecer da AEPD sobre “Corresponder aos desafios dos Grandes Volumes de Dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade”, 2015.

6. CONCLUSÕES

Em face do exposto, salientam-se as seguintes ideias referentes às matérias abordadas em cada capítulo.

Com a globalização dos mercados, são recolhidos e tratados volumes maciços de dados pessoais. Esta utilização representa graves riscos para a privacidade das pessoas e para a proteção dos seus dados pessoais, enquanto informações relativas a pessoas identificadas ou identificáveis. Atualmente, os dados pessoais passam a ser encarados como uma “matéria-prima”.

Os avanços tecnológicos já ultrapassaram os quadros legais existentes, criando tensão entre a inovação e a privacidade, sempre que as leis não refletem os novos contextos sociais e não garantem os direitos dos cidadãos. Torna-se essencial encontrar novas configurações jurídicas que respondam aos desafios desta realidade.

Assim, “a *Internet* é uma bênção e uma maldição ao mesmo tempo”!²²⁴

Concluimos que a *Internet* não deve ser hiper-regulada, mas também não deve ser, simplesmente, “autorregulada”. Tendo em conta os modelos sugeridos de regulação da *Internet*, é possível defender um modelo constituído por elementos comuns a diferentes planos de regulação, sem abdicar, nunca, do papel do Direito.

Da mesma forma, não deve considerar-se que não pode existir privacidade no mundo digital. As regras que visam a proteção de dados aplicam-se, assim, a qualquer veículo de informação e comunicação, suscitando, porém, a *Internet* difíceis desafios tendo em conta a sua natureza desmaterializada.

A privacidade informacional e a proteção de dados são construções jurídicas, correspondentes a direitos, liberdades e garantias, que visam o combate à transformação da “pessoa” em “objeto”. Neste direito geral à proteção de dados estão incluídas diversas posições jurídicas, que se consubstanciam em direitos, deveres e garantias.

²²⁴ BLUME, Peter – *Op. cit.*, 2015, p. 11.

O direito à proteção de dados consiste no direito que cada indivíduo tem de controlar a sua exposição na sociedade e garantir a sua privacidade. É um direito fundamental intrínseco ao ser humano.

O regime europeu de proteção de dados é suficientemente amplo para englobar todos os tipos de tratamento de dados pessoais, incluindo no quadro da *Internet*.

A *Internet* ignora e questiona a soberania e a jurisdição dos Estados. Daí que a proteção de dados pessoais dos cidadãos europeus só possa ser eficaz se os níveis de proteção fora da Europa forem idênticos aos europeus. A nível da *Internet*, na medida em que a sua utilização e a evolução das TIC têm tomado proporções avassaladoras, a regulação da proteção de dados através da Diretiva 95/46/CE encontrava-se, em larga medida, ultrapassada.

A reforma europeia, encetada a 25 de janeiro de 2012 e que inclui o Regulamento Geral de proteção de dados, tem como objetivos reforçar as regras de privacidade e de proteção de dados, expor os desafios estruturais de aplicar o paradigma da proteção de dados à *Internet*, especialmente no que toca à definição de “dado pessoal” e à aplicação extraterritorial do Direito da UE. A expectativa é que o pacote de reformas de proteção de dados da UE fortaleça e modernize a moldura regulatória.

Esta força provém, desde logo, do facto de a regulação deste direito ser realizada através de um Regulamento, o que comprova o alto nível de proteção conferida a esta matéria, uma vez que este instrumento se aplica diretamente na ordem jurídica dos Estados-Membros da UE e atua enquanto Direito supranacional, de acordo com o princípio do primado do Direito da UE.

A distinção entre o direito à privacidade e o direito à proteção de dados também se afere pelo facto de a Diretiva, à semelhança da Convenção n.º 108 do Conselho da Europa, estabelecer no n.º 1 do art. 1.º o objetivo de defesa dos direitos e liberdades fundamentais, em particular o direito à vida privada, enquanto o novo Regulamento institui como seu objetivo a defesa dos direitos e liberdades fundamentais, mas, em especial, o direito à proteção dos dados pessoais.

Nesta reforma, assinalam-se diversas transformações relativamente ao anterior regime de proteção de dados. Assim, protege-se um direito que é formalmente “não-preocupado” com uma tecnologia específica e representa-se este direito como um verdadeiro direito fundamental da UE.

Uma das inovações do regime da UE para que se proteja a proteção de dados de um modo mais efetivo passa por se proteger, tecnologicamente, a privacidade dos dados, não apenas “por defeito”, mas também “desde a conceção” das TIC.

Uma efetiva proteção de dados é assegurada por estas medidas e por um maior controlo dos dados pelo seu titular, através de uma maior transparência quanto às políticas de tratamento de dados pessoais.

O Regulamento reforça a proibição de tratamento de dados sensíveis, consagrando algumas exceções nas quais o mesmo é permitido. Contudo, até mesmo quanto aos direitos dos titulares dos dados, existem limitações possíveis, desde que respeitem a essência dos direitos e liberdades fundamentais e constituam uma medida necessária e proporcionada numa sociedade democrática para assegurar diversos valores, elencados no art. 23.º.

Apesar destes avanços, há sempre certas garantias legais para a privacidade e a proteção de dados pessoais que precisam de ser reforçadas pelos desafios colocados pela tecnologia e globalização, constantemente maiores e mais difíceis de ultrapassar.

Da mesma forma, devemos ter presente que a proteção dos dados pessoais passa, também, pela consciencialização do próprio utilizador da *Internet*, o qual deve estar atento aos termos relativos ao uso e à privacidade no contexto dos serviços *online* e deve limitar-se quanto ao que partilha neste mundo digital, tendo sempre em conta que os seus dados podem ser recolhidos e tratados, mesmo sem o seu conhecimento. Aliás, seria, até, conveniente que os utilizadores da *Internet* recebessem uma formação adequada sobre o teor dos seus direitos à privacidade e à proteção de dados e aos meios de defesa ao seu dispor.

Deste modo, torna-se também relevante a cooperação entre os Estados-Membros e com países terceiros, de modo a enraizar regras e práticas comuns no que toca ao

fluxo transfronteiriço de dados e às normas de proteção dos dados. Isto, uma vez que continua a haver variações, diferenças e conflitos entre as soberanias nacionais sobre a natureza, tradição, abordagem e mecanismos de proteção de dados, o que pode complicar as situações das empresas que se pretendam sediar num Estado distinto do de origem. Enquanto não se coloca uma legislação internacional uniforme na agenda, não se deve negligenciar as colaborações bilaterais, regionais e multilaterais entre os Estados sobre a proteção transfronteiriça de dados.

Em conclusão, a evolução da Sociedade da Informação tem de ser, constantemente, acompanhada por regras de proteção de dados que se adequem aos novos desafios colocados pelo avanço destas tecnologias e pela utilização, cada vez mais acentuada, da *Internet*. É necessário encetar esforços no sentido de possibilitar a progressão digital, protegendo, simultaneamente, os direitos fundamentais.

A proteção de dados na UE precisa de ser digital: efetiva na prática, dinâmica e amiga do utilizador, com ênfase não nos procedimentos, mas em salvaguardas reais para os indivíduos.

Como já referido pela AEPD, devemos aproveitar a oportunidade de uma economia global digital, mas de forma sustentável, ou seja, através da redefinição de princípios para proteção de direitos fundamentais no mundo digital, do reforço do poder dos indivíduos *online*, de um maior respeito pelos direitos dos indivíduos neste campo, e de um fortalecimento da cooperação europeia e internacional no que concerne a esta temática.

Não restam, assim, dúvidas de que o direito à proteção de dados se tenha consagrado como um verdadeiro direito fundamental, autónomo quanto ao direito à privacidade. Esta consideração é fundamentada na atual legislação de proteção de dados, nomeadamente o Regulamento Geral, e pela jurisprudência do TJ, o qual se refere, especificamente, ao “direito fundamental à proteção de dados”, em diversos dos seus Acórdãos.

“O direito a não ser importunado é verdadeiramente o começo de toda a liberdade”

²²⁵ “*The right to be let alone is indeed the beginning of all freedom*” - Voto vencido do juiz William Orville Douglas no caso *Public Utilities Commission v. Pollak*, 343 U.S. 451-467, 1952.

7. REFERÊNCIAS BIBLIOGRÁFICAS

A. Monografias, Obras Coletivas e Artigos em Publicações Periódicas:

- ✚ ABRAHAMSON, Zachary - Essential Data. *In: The Yale Law Journal*, Vol. 124, 2014, pp. 867–881. ISSN: 0044-0094.
- ✚ ANDRADE, José Carlos Vieira – Os Direitos Fundamentais na Constituição Portuguesa de 1976. Coimbra: Almedina, 4.^a ed., 2009. ISBN: 978-972-40-3716-5.
- ✚ ANTUNES, Luís Filipe - A privacidade no mundo conectado da Internet das coisas. *In: Fórum de Protecção de Dados*, n.º 2, pp. 52–58. Lisboa, 2016.
- ✚ ASCENSÃO, José de Oliveira - Estudos sobre direito da Internet e da sociedade da informação. Coimbra: Almedina, 2001. ISBN: 972-40-1501-7.
- ✚ BENEDEK, Wolfgang (ed.) - Understanding Human Rights Manual on Human Rights Education. Viena: European Training and Research Centre for Human Rights and Democracy, 3.^a ed., 2012. ISBN: 978-1-78068-057-6.
- ✚ BLUME, Peter – Is is Time for Tomorrow: EU Data Protection Reform and the Internet. *In: Journal of Internet Law*, Vol. 18, n.º 8, 2015, p. 3-13. ISSN: 1094-2904.
- ✚ BURKERT, Herbert - General Report Standards Applicable to the Internet: Benefits and Limitations: “Internet and the Law – Disturbances and Early Sorrow”. *In: CHATILLON, Georges (Ed.) - Internet International Law: International and European Studies and Comments*. Bruxelas: Bruylant, 2005, pp. 211-219. ISBN: 2-8027-1743-X.
- ✚ BYGRAVE, Lee A. – Data privacy law and the Internet: policy challenges. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 259-289. ISBN: 978-1-107-04167-7.
- ✚ CALVÃO, Filipa – O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento. *In: Fórum de Protecção de Dados*, n.º 1, 2015, pp. 37-48. P. 44.

- ✚ CAMPOS, João Mota, CAMPOS, João Luís Mota e PEREIRA, António Pinto – Manual de Direito Europeu. Coimbra: Coimbra Editora, 2014, 7.^a ed.. ISBN: 978-972-32-2209-8. P. 278.
- ✚ CANOTILHO, José Joaquim Gomes – Direito Constitucional e Teoria da Constituição, 7.^a edição (10.^o reimpressão). Coimbra: Almedina, 2003. ISBN: 978-972-40-2106-5.
- ✚ CANOTILHO, José Gomes e MOREIRA, Vital – Constituição da República Portuguesa Anotada, Vol. I, 4.^a ed. revista. Coimbra: Coimbra Editora, 2007. ISBN: 978-972-32-1462-8.
- ✚ CASTRO, Catarina Sarmento - Direito da Informática, Privacidade e Dados Pessoais. Coimbra: Almedina, 2005. ISBN 972-40-2424-5.
- ✚ CASTRO, Catarina Sarmento - Protecção de dados pessoais na Internet. **Sub Judice. Justiça e Sociedade**, n.º 35, Set. 2006, pp. 11-29. ISSN: 978-972-40-2999-3.
- ✚ CHATILLON, Georges – Presentation. *In*: CHATILLON, Georges (Ed.) - **Internet International Law: International and European Studies and Comments**. Bruxelas: Bruylant, 2005, pp. 7-41. ISBN: 2-8027-1743-X.
- ✚ Comissão Europeia - Para uma Europa do Conhecimento. A União Europeia e a Sociedade da Informação. **Série: A Europa em Movimento**. Luxemburgo, 2003. ISBN: 92-894-4426-6.
- ✚ Conselho da União Europeia – Carta dos Direitos Fundamentais da União Europeia: Anotações relativas ao texto integral da Carta. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 2001. ISBN: 92-824-1959-2.
- ✚ DONEDA, Danilo - A Proteção Dos Dados Pessoais Como Um Direito Fundamental. *In*: **Espaço Jurídico**, v. 12, n.o 2, jul./dez. 2011, pp. 91-108. ISSN: 2179-7943.
- ✚ FARIA, Miguel José – Direitos Fundamentais e Direitos do Homem, Vol. I, 3.^a ed. revista e ampliada. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2001. ISBN: 972-8630-03-4.
- ✚ FINK, Udo – Protection of privacy in the EU, individual rights and legal instruments. **Emerging challenges in privacy law: comparative**

perspectives. Cambridge: Cambridge University Press, 2014, pp. 75-91. ISBN: 978-1-107-04167-7.

- ✚ FRAYSSINET, Jean - Is protection of Personal Data guaranteed on the Internet? *In: CHATILLON, Georges (Ed.) - Internet International Law: International and European Studies and Comments.* Bruxelas: Bruylant, 2005, pp. 421-429. ISBN: 2-8027-1743-X.
- ✚ FUSTER, Gloria González - The Emergence of Personal Data Protection as a Fundamental Right of the EU. Londres: Springer Ed.. ISBN 978-3-319-05023-2.
- ✚ GONÇALVES, Maria Eduarda – Direito da Informação: Novos direitos e formas de regulação na Sociedade da Informação. Coimbra: Almedina, 2003. ISBN: 972-40-1908-X.
- ✚ GOUVEIA, Jorge Bacelar - Os Direitos Fundamentais à Protecção dos Dados Pessoais Informatizados. *In: Revista da Ordem dos Advogados*, Ano 51-III, 1991, pp. 700-732. ISSN: 0870-8118.
- ✚ GREENLEAF, Graham - A world data privacy treaty? ‘Globalisation’ and ‘modernisation’ of Council of Europe Convention 108. **Emerging challenges in privacy law: comparative perspectives**, pp. 92-140. Cambridge: Cambridge University Press, 2014. ISBN: 978-1-107-04167-7.
- ✚ HERT, Paul e GUTWIRTH, Serge – Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. *In: GUTWIRTH, S., POULLET, Y., HERT, P., TERWANGNE, C. e NOUWT, S. (Ed.) - Reinventing Data Protection*, Cap. 1. Heidelberg: Springer, 2009. ISBN: 978-1-4020-9497-2.
- ✚ HERT, Paul e PAPAKONSTANTINO, Vagelis - The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *In: Computer Law & Security Review*, n.º 28, Issue 2, 2012, pp. 130-142. ISSN: 0267-3649.
- ✚ HORNUNG, Gerrit e SCHNABEL, Christoph – Data protection in Germany I: The population census decision and the right to informational self-determination. *In: Computer Law & Security Report*, Vol. 25, Issue 1, 2009, pp. 84-88. ISSN: 0267-3649.

- ✚ KONG, Lingjie – Data Protection and Transborder Data Flow in the European and Global Context. *In: European Journal of International Law*, V. 21, *Issue* 2, 2010, pp. 441-456. ISSN: 0938-5428.
- ✚ LINDSAY, David - The «right to be forgotten» in European data protection law. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 290–337. ISBN 978-1-107-04167-7.
- ✚ LOPES, Joaquim de Seabra – O artigo 35.º da Constituição: Da Génese à Atualidade e ao Futuro Previsível. *In: Fórum de Proteção de Dados*, n.º 2, 2016, pp. 14-49.
- ✚ MILT, Kristiina - Proteção dos Dados Pessoais. Parlamento Europeu - Fichas técnicas sobre a União Europeia, 2017. Disponível em: http://www.europarl.europa.eu/ftu/pdf/pt/FTU_5.12.8.pdf (Consultado a 06/06/2017).
- ✚ MONIZ, Helena – Notas sobre a Protecção de Dados Pessoais perante a Informática (O caso especial dos dados pessoais relativos à saúde). *In: Revista Portuguesa de Ciência Criminal*, Ano 7, Fasc. 2.º, Abril-Junho 1997, pp. 231-298. ISSN: 0871-8563.
- ✚ MOREHAM, Nicole – Protection against intrusion in English legislation. **Emerging challenges in privacy law: comparative perspectives**, pp. 141-156. Cambridge: Cambridge University Press, 2014. ISBN: 978-1-107-04167-7.
- ✚ OLIVEIRA, Bárbara Nazareth, GOMES, Carla de Marcelino e SANTOS, Rita Páscoa dos - Os Direitos Fundamentais em Timor-Leste: Teoria e Prática. Coimbra: *Ius Gentium Conimbrigae* — Centro de Direitos Humanos da Faculdade de Direito da Universidade de Coimbra, 2015. ISBN: 978-989-20-5236-6.
- ✚ PINHEIRO, Alexandre Sousa - *Privacy* e proteção de dados pessoais: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL, Ed., 2015. ISBN: 978-612-00-0260-5.
- ✚ POULLET, Yves – Views from Brussels: A European Internet Law. CHATILLON, Georges (Ed.) - **Internet International Law: International and European Studies and Comments**. Bruxelas: Bruylant, 2005, pp. 123-165. ISBN: 2-8027-1743-X.


- ✚ ROBINSON, Neil, GRAUX, Hans, BOTTERMAN, Maarten e VALERI, Lorenzo - Review of the European Data Protection Directive. Cambridge: Rand Corporation, 2009. P. 7. Disponível em: https://www.rand.org/pubs/technical_reports/TR710.readonline.html. (Consultado a 06/06/2017).
- ✚ SHAPIRO, Andrew L. – The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know. Nova Iorque: PublicAffairs, 1999. ISBN: 1-891620-86-X.
- ✚ SILVEIRA, Luís Lingnau da - A Protecção de dados pessoais na Internet. *In: Europa: Novas Fronteiras*, n.º 28-29, janeiro/dezembro 2011, pp. 139-143. ISSN: 0873-8068.
- ✚ TILBURY, Michael – Privacy: Common Law or Human Right. **Emerging challenges in privacy law: comparative perspectives**. Cambridge: Cambridge University Press, 2014, pp. 157-179. ISBN: 978-1-107-04167-7.
- ✚ VASCONCELOS, Pedro Pais – Protecção de Dados Pessoais e Direito à Privacidade. **Direito da Sociedade da Informação e Direito de Autor**, V. I, 1999, pp. 241-253. ISBN: 978-972-32-2167-1.
- ✚ VAZ, Ana - Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais. *In: Nação e Defesa*, n.º 117, 3.ª Série, 2007, pp. 35-63. ISSN: 0870-757X.
- ✚ VICENTE, Dário Moura - Direito Internacional Privado: Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005. ISBN: 972-40-2641-8.
- ✚ WARREN, Samuel e BRANDEIS, Louis - The Right to Privacy. *In: Harvard Law Review*, vol. IV, n.º 5, Dez. 1890 ISSN: 0017-811X.
- ✚ WITZLEB, Normann, LINDSAY, David, PATERSON, Moira e RODRICK, Sharon – An overview of emerging challenges in privacy law. **Emerging challenges in privacy law: comparative perspectives**, pp. 1-28. Cambridge: Cambridge University Press, 2014. ISBN: 978-1-107-04167-7.

B. Recursos eletrônicos:


-  <https://icdppc.org/>
-  <https://oecd.org/sti/ieconomy/privacy-guidelines.htm>
-  <http://eur-lex.europa.eu/>
-  <http://hudoc.echr.coe.int/>
-  <http://www.pgdlisboa.pt/>
-  <https://dre.pt/>
-  <http://coe.int/en/web/conventions/>
-  <https://treaties.un.org/>
-  <https://curia.europa.eu/>
-  <http://europarl.europa.eu/>
-  <http://hudoc.echr.coe.int/>

C. Documentos:

ONU:

-  Alto Comissariado das Nações Unidas para os Direitos Humanos - Relatório “O Direito à Privacidade na Idade Digital”. Resolução n.º 68/167, de 18 de dezembro de 2013. Documento A/RES/68/167. Disponível em: <https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf> (Consultado a 06/06/2017).

OCDE:

-  OCDE – Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, de 1980. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofprivacyandtransborderflowsofpersonaldata.htm> (Consultado a 06/06/2017).

Conselho da Europa:

- ✚ Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 1981. Disponível em <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> (Consultado a 06/06/2017).

União Europeia:

-- Legislação:

- ✚ Carta dos Direitos Fundamentais da União Europeia, assinada e proclamada no Conselho Europeu de Nice de 7 de dezembro de 2000. Publicada no Jornal Oficial n.º C202, de 07/06/2016, pp. 389-405.
- ✚ Decisão-Quadro 2008/977/JAI do Conselho, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. Publicada no Jornal Oficial n.º L350/60, de 30/12/2008. Esta Decisão-Quadro foi, entretanto, revogada pela Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
- ✚ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, publicada no Jornal Oficial n.º L281/31, de 23/11/95. Transposta através da Lei n.º 67/98 de 26/10/1998, publicado no Diário da República, 1.ª Série A, n.º 247, de 26/10/1998. Última alteração pela Lei n.º 103/2015, de 24/08/2015.
- ✚ Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações. Publicada no Jornal Oficial n.º L24, de 30/01/1998, pp. 1-8. Transposta pela Lei n.º 69/98, de 28/10/1998, publicada no Diário da República, 1.ª Série A, n.º 249, de 28/10/1998, p. 5572.
- ✚ Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas. Publicada no Jornal Oficial n.º L201, 31/07/2002, pp. 37-47. Transposta pelo Decreto-Lei n.º 7/2004, de 07/01/2004, publicada no Diário da República, 1.ª Série A, n.º 5, de 07/01/2004, p. 70.

- + Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicada no Jornal Oficial n.º L119/89, de 04/05/2016.
- + Memorando Explicativo da Carta. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF> (Consultado a 06/06/2017).
- + Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicado no Jornal Oficial n.º L119/1, de 04/05/2016.
- + Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de dezembro de 2007. Publicado no Jornal Oficial n.º C306, de 17/12/2007, pp. 1-271.

-- Comunicações, Pareceres, Relatórios e Resoluções:

- + Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia. Documento: COM(2010) 609 final. Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (Consultado a 06/06/2017).
- + Comunicação da Comissão ao Conselho: Uma Política Comunitária de Tratamento de Dados. Documento: SEC(73) 4300 final, disponível em: <http://aei.pitt.edu/6337/1/6337.pdf> (Consultado a 06/06/2017).
- + Comunicação da Comissão Europeia ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre “Uma abordagem compreensiva sobre a protecção de dados pessoais na União Europeia”. Documento: COM(2010) 609 final, de 4 de novembro de 2010.
- + Parecer do Comité Económico e Social Europeu sobre a “Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia”, n.º 2011/C 248/21. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52011AE0999&from=EN> (Consultado a 06/06/2017).

- ✚ Parecer da AEPD respeitante à Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados. Publicado no Jornal Oficial n.º C255/01, de 27/10/2007.
- ✚ Parecer da AEPD sobre “Corresponder aos desafios dos Grandes Volumes de Dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade” (2016/C 67/05), de 20 de fevereiro de 2015.
- ✚ Parecer da AEPD sobre a promoção da confiança na sociedade da informação através do reforço da protecção dos dados e da privacidade (2010/C280/01), de 16 de outubro de 2010.
- ✚ Recomendação da AEPD sobre as opções da União Europeia para a reforma da proteção de dados, n.º 2015/C 301/01. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2015:301:FULL&from=EN> (Consultado a 06/06/2017).
- ✚ Recomendação da Comissão n.º 81/679/CEE, relativa a uma convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, publicada no Jornal Oficial n.º L246/31, de 29/08/1981, p. 77.
- ✚ Relatório da Agência da União Europeia para a Segurança das Redes e da Informação “*The right to be forgotten – between expectations and practice*”. Heraclião: ENISA. P. 14. Disponível em: <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten> (Consultado a 06/06/2017).
- ✚ Resolução do Parlamento Europeu sobre a proteção dos direitos do indivíduo face aos desenvolvimentos tecnológicos no campo do tratamento automático de dados, 1975, publicada no Jornal Oficial n.º C60/48; e Resolução do Parlamento Europeu de 8 de abril de 1976 sobre a proteção dos direitos do indivíduo face aos desenvolvimentos tecnológicos no campo do tratamento automático de dados, 1976, publicada no Jornal Oficial n.º C100/27.

- ✚ Resolução do Parlamento Europeu sobre a proteção do indivíduo face a desenvolvimentos tecnológicos no tratamento de dados, publicada no Jornal Oficial n.º C87, de 09/03/1982, pp. 39-41.
- ✚ Resolução sobre a proteção dos direitos do indivíduo face a desenvolvimentos tecnológicos no tratamento de dados, adotada a 8 de maio de 1979, publicada no Jornal Oficial n.º C140, de 05/06/1979, pp. 34-38.
- ✚ *Working Document of European Parliament*, Documento 1-42/83, Março 1983, p. 2. Disponível em http://aei.pitt.edu/59917/1/EPWD-2_B3_52.pdf (Consultado a 06/06/2017).

Portugal:

- ✚ Lei n.º 10/91 de 29 de abril, a Lei da Protecção de Dados Pessoais face à Informática. Publicada no Diário da República, 1.ª Série A, n.º 98, 1991-04-29, pp. 2366-2372.
- ✚ Lei n.º 67/98, de 26 de outubro, Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). Publicada no Diário da República, 1.ª Série A, n.º 247/1998, de 26/10/1998.
- ✚ Resolução da Assembleia da República n.º 39/2013, de 3 de abril de 2013. Publicada no Diário da República n.º 65/2013, Série I de 2013-04-03, p. 1950.

D. Jurisprudência:

Tribunal de Justiça da União Europeia:

- ✚ Acórdão *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, relativo ao Processo C-131/12.
- ✚ Acórdão *Lindqvist*, de 6 de novembro de 2003, no âmbito do Processo C-101/01.
- ✚ Acórdão *Promusicae v. Telefónica de España SAL*, de 29 de janeiro de 2008, relativo ao Processo C-275/06.

- ✚ Acórdão *Rundfunk*, de 20 de maio de 2003, relativo aos Processos Apensos C-465/00, C-138/01 e C-139/01.
- ✚ Conclusões da Advogada-Geral Eleanor Sharpston apresentadas em 17 de junho de 2010, no âmbito do Acórdão *Schecke E Eifert*, relativo aos Processos Apensos C-92/09 E C-93/09.

Tribunal Europeu dos Direitos do Homem:

- ✚ Caso *Gaskin v. The United Kingdom*, de 7 de julho de 1989, Processo n.º C(89) 90.
- ✚ Caso *Khelili v. Switzerland*, de 18 de outubro de 2011, Processo n.º 195(2011).

Tribunais Nacionais:

-- Portugal:

- ✚ Acórdão do Tribunal Constitucional n.º 182/89, de 2 de março de 1989. Decorrente do Processo n.º 298/87, disponível em: <http://publicos.pt/documento/id612862/acordao-182/89> (Consultado a 06/06/2017).

-- Alemanha:

- ✚ Caso “*The Population Census Decision*”, *Bundesverfassungsgericht*, Tribunal Constitucional Federal da Alemanha, de 1984. Disponível em: <http://www.servat.unibe.ch/dfr/bv065001.html> (Consultado a 06/06/2017).

E. Discursos:

Autoridade Europeia para a Proteção de Dados:

BUTTARELLI, Giovanni - Ethics at the Root of Privacy and as the Future of Data Protection. 2016.

BUTTARELLI, Giovanni - The General Data Protection Regulation: Making the world a better place? Discurso em “*EU Data Protection 2015 Regulation Meets Innovation*”, São Francisco, 2015.

Referências Bibliográficas

BUTTARELLI, Giovanni - Value of the EU Data Protection Reform against the Big Data challenges. 5th European Data Protection Days, Berlim, 2015.

HUSTINX, Peter – “Ensuring more effective data protection in an age of big data”. Contribuição para “*European Voice online debate on big data and consent*”, 2014. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-07-14_ph_for_ev_online_en.pdf (Consultado a 06/06/2017).

ÍNDICE

Declaração de Compromisso de Anti- Plágio.....	i
Agradecimentos.....	iii
Modo de Citar e Outros Esclarecimentos.....	iv
Lista de Abreviaturas, Siglas e Acrónimos	v
Declaração de Conformidade do Número de Caracteres	vii
Resumo.....	viii
Abstract	ix
1. Introdução.....	1
2. Relação entre o Ciberespaço e o Direito	5
2.1. Evolução Tecnológica e modelos de regulação jurídica do ciberespaço.....	5
2.2. A Privacidade é um mito na Internet?.....	9
3. Fontes jurídicas do direito à proteção de dados pessoais.....	13
3.1. Fontes de Direito Internacional	15
3.1.1. Organização das Nações Unidas (ONU).....	15
3.1.1.1. Declaração Universal dos Direitos Humanos e Pactos.....	16
3.1.1.2. Diretrizes Para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal.....	16
3.1.1.3. Direito à proteção de dados pessoais como Direito Humano no âmbito da ONU.....	16
3.1.2. Organização para a Cooperação e Desenvolvimento Económico (OCDE)	17
3.1.2.1. Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.....	17
3.1.2.2. Direito à proteção de dados pessoais como Direito Humano no âmbito da OCDE.....	18
3.1.3. Conselho da Europa	18
3.1.3.1. Convenção Europeia dos Direitos do Homem (CEDH) e Jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH)	19
3.1.3.2. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal	20
3.1.3.3. Direito à proteção de dados pessoais como Direito Humano no âmbito do Conselho da Europa	21
3.2. Fontes de Direito da União Europeia (UE)	22

3.2.1. Tratados e Carta dos Direitos Fundamentais da UE	22
3.2.2. Instrumentos Relevantes até à adoção da Diretiva 95/46/CE	25
3.2.3. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro 29	
3.2.4. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados)	33
3.2.5. Direito à proteção de dados pessoais como Direito Fundamental no âmbito da UE.....	36
3.3. Fontes de Direito Nacional.....	38
3.3.1. Constituição da República Portuguesa.....	38
3.3.2. Lei n.º 10/91, de 29 de abril e Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais face à Informática).....	42
3.3.3. Direito à proteção de dados pessoais como Direito Fundamental no âmbito nacional	44
4. Enquadramento ao direito à proteção de dados pessoais no Regulamento Geral	46
4.1. Conceito do direito à privacidade e evolução até à autonomização do direito à proteção de dados	46
4.1.1. Conceito e evolução do direito à privacidade	46
4.1.2. Distinção entre direito à privacidade e direito à proteção de dados.....	52
4.1.4. Posição adotada.....	58
4.2. Conceito e categorias de dados pessoais	60
4.2.1. Noção de dados pessoais	60
4.2.2. Diferentes categorias de dados pessoais	63
4.2.3. Conceito de tratamento de dados pessoais	64
4.2.4. Posição adotada.....	69
5. Direito à proteção de dados pessoais no Regulamento Geral.....	70
5.1. Evolução do direito à proteção de dados pessoais como Direito Fundamental da Diretiva 95/46/CE até ao novo Regulamento Geral da UE	70
5.2. Atual Regime de Proteção de Dados na UE	77
5.3. Direito Fundamental à proteção de dados pessoais no Regulamento Geral.....	81
5.2.1. Princípios orientadores da proteção de dados	82
5.2.2. Conteúdo do direito à proteção de dados	85
5.2.2.1. Direitos dos titulares de dados pessoais	85
A) Direito ao conhecimento.	87
B) Direito de informação.	88

C) Direito de acesso.....	88
D) Direito de retificação	89
E) Direito ao apagamento dos dados (“direito a ser esquecido”).....	90
F) Direito à limitação do tratamento.....	93
G) Direito de portabilidade dos dados.....	93
H) Direito de oposição.....	93
I) Direito de não ficar sujeito a decisões individuais automatizadas.....	94
5.2.2.2. Deveres dos responsáveis de tratamento de dados pessoais.....	96
6. Conclusões.....	99
7. Referências Bibliográficas	104